Votiro Disarmer

User Guide

Version 8.4

July, 2021

Copyright Notice

www.votiro.com

Contents

1 Introduction

1.1 Votiro's Disarmer Technology

Votiro Disarmer secures your organization by eliminating threats that enter your network from known and unknown sources. Votiro Disarmer ensures that files and emails from any source and in any format are neutralized or blocked before they reach the organization's network.

Votiro Disarmer protects your organization from all sources of file exploit attempts that are processed through various channels such as email, file shares, web downloads, or any supported custom application. Votiro Disarmer is enterprise-oriented, easy to integrate, and seamless. It also eliminates the reliance on users' assessment of the safety of incoming emails or files.

Votiro Disarmer implements a multi-layer security mechanism that integrates several critical components to eliminate cyber threats that attempt to penetrate an organization.

Votiro Disarmer is deployed as a set of Windows Services.

1.1.1 True Type Detection

True Type Detection (TTD) determines a file's type by comparing the extension associated with the file with the specifications dictated by the vendor for that file type. For example, Microsoft Corporation has specified that a file with the extension .docx is a Microsoft Word document. In order for Word to open the file correctly, the file attributes must meet specific criteria designated by Microsoft. TTD verifies the criteria set by Microsoft are met before the file is processed.

When TTD is used in the Votiro Disarmer solution and specified by the applied policy, files with content that does not match the file extension criteria can be blocked to prevent malicious content exploits.

1.1.2 Virus Detection

Virus detection is provided by several integrated third-party antivirus engines. Standard virus detection uses a signature database file of known viruses that is regularly updated by the vendors of integrated engines. The virus detection engine compares new files entering the network against the signature database, to search for existing viruses. The signature file must be updated regularly via an Internet connection. If the signature file is out of date, the detection of known threats might be degraded.

Votiro Disarmer includes a number of the most accurate and reliable antivirus engines, to integrate a broad spectrum of virus detection on your incoming files.

1.1.3 Content Disarm and Reconstruction (CDR)

Votiro's patented and award-winning products use next-generation CDR technology to identify and disarm malware from incoming files, then reconstruct

them, while preserving the integrity and functionality of the original data before reaching your premises – all in less than 1 second.

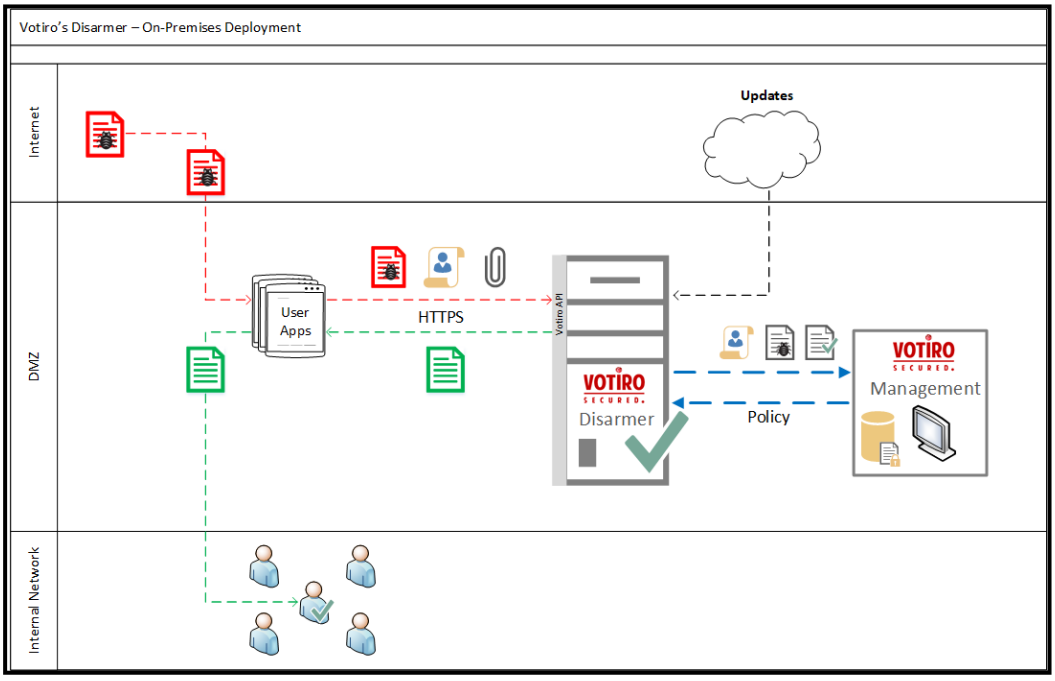
Votiro's proprietary technology allows users to safely open email attachments, download and transfer files, share content, and use removable devices – all without giving it a second thought. Supporting mobile and desktop editions of a vast arsenal of file types, including Microsoft Office, RTF, PDF (such as Adobe PDF), image, and archive files, Votiro's CDR technology provides automatic defense, removing the human factor from the security process.

Threat sanitization is achieved through micro changes to the structure and metadata of a file. Invisible to users, these changes do not affect the file's usability but eliminate the possibility of malicious code being run from the file, thereby neutralizing the threat.

By actively processing all files, without having to detect threats in advance, Votiro protection surpasses standard methods and removes undisclosed, advanced threats before they penetrate an organization.

1.2 System Architecture and Data Flow

A general view of the Disarmer product in relation to other key elements in the network is provided in the following diagram:

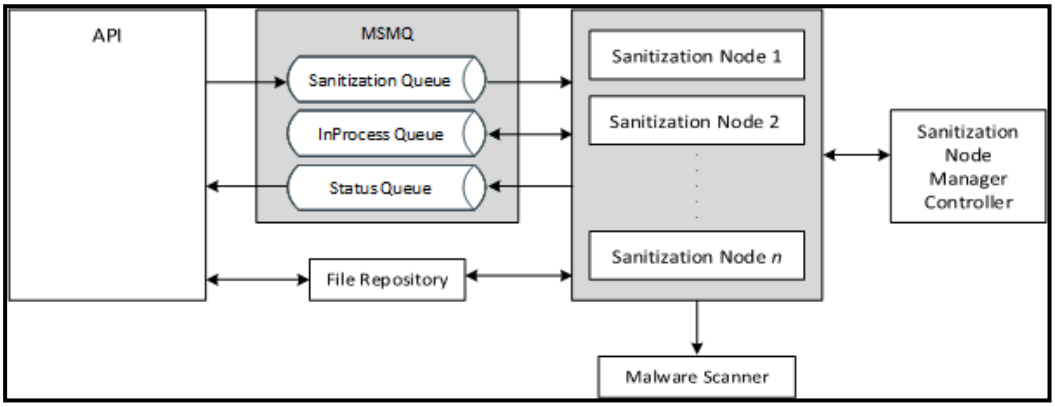


Data flows between the user application (Votiro Disarmer API consumer) and Disarmer. Communication consists of multiple bi-directional messages that include queuing, tracking, and file transfers.

The Votiro Disarmer engine is at the heart of the Votiro sanitization solution. The engine is provided with a front-end Management consule that is used for the following:

- Monitoring and analyzing sanitization activity in the Disarmer engine.
- Creating and editing sanitization policies that are regularly updated in the Disarmer engine.
- Storing metadata that describes the files, along with the original and sanitized files themselves for incident management and zero-day identification.

The next diagram shows how sanitization requests flow between the Disarmer API and the Disarmer Sanitization Nodes, which are managed by the Sanitization Node Manager Controller (SNMC).



- A sanitization request enters the system via the API service: a sanitization request for the file is queued in the Sanitization Queue, while the file to be sanitized is still in the File Repository.
- The SNMC is the sanitization system watchdog. It performs a health check by polling the nodes every defined time period (depending on the configuration) to ensure that there are n sanitization node processes running at any time.
- The maximum number of sanitization nodes running at any time equals the number of processor cores in the computer where Disarmer is running, provided the available memory per node is no less than 2 GB.
- Should the SNMC detect that any node is non-responsive (because it has crashed or hanged), it terminates that node and spawns a new one in its place.
- Each node polls the Sanitization Queue for a new incoming request, which is a reference containing the file name in the File Repository.
- When a request comes to the top of the Sanitization Queue, the next available node pulls the reference from the queue and accesses the referenced file in the File Repository to begin the sanitization process.
- After sanitization begins, it is stored in the InProcess Queue for status tracking and each status update is queued in the Status Queue. Status updates are polled by the API service and reflected to the user.

- As part of the sanitization, the node passes the file to the Votiro Scanner service for antivirus scanning.

1.3 Supported File Types

The following table lists the file types and attributes supported by Votiro Disarmer. The information is arranged according to the categories that appear in the Action by File Type area of the Policies page in the Votiro Management Dashboard.

- Types marked with ^ are scanned by the AV engines and their true file type is verified based on their structure. The files are not modified by this process.
- Types Types marked with ** are obsolete, are not recommended as filters in a production environment. Support for these types might be discontinued in a later version.

Table 1 File Types

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
PDF	PDF	Adobe PDF	pdf	
Image	Animated GIF	Raster Image Files	gif	
	BMP	Raster Image Files	bmp	rle
	EMF	Vector Image Files	emf	
	GIF	Raster Image Files	gif	
	JPEG	Raster Image Files	jpeg	jpg, emf, wmf, jp2
	PNG	Raster Image Files	png	emf
	Portable Gray Map Image File ** ^	Raster Image Files	pgm	
	PPM File ** ^	Raster Image Files	ppm	
	TIF	Raster Image Files	tif	tiff
	WDP	Raster Image Files	Wdp	
	WMF	Vector Image Files	wmf	
CAD	DWG File	CAD Files	dwg	
	DWS File	CAD Files	dws	
	DWT File	CAD Files	dwt	
	DXF File	CAD Files	dxf	
	JWW File	CAD Files	jww	
	P21 File	CAD Files	p21	
	Sfc File	CAD Files	sfc	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
Ichitaro	JTD File	Ichitaro Files	jtd	
	JTDC File	Ichitaro Files	jtdc	
Hancom	HWP File	Hancom Files	hwp	
Binary	Binary File ^	Any Binary Files	dat	db
	Executable ^	Any Binary Files	exe	com, dll, pif, sfx, msu, msp, msi, mo
Archive	7Z File	Archives	7z	
	CAB file	Archives	cab	wsp
	GZ File	Archives	gz	
	GZIP File	Archives	gzip	
	InstallShield CAB file ^	Archives	cab	
	LZH File ^	Archives	lzh	
	RAR File	Archives	rar	Including RAR5
	Tar File	Archives	tar	
	VMware Virtual Machine Disk ^	Archives	vmdk	
	ZIP File	Archives	zip	
RTF	RTF Files	RTF Files	rtf	
Email	Calendar File	Calendar Files	ics	
	DAT File ** ^	EML Files	dat	
	EML File	EML Files	eml	tmp
	HTML Body ^	HTML Files	html	htm
	MSG File	MSG Files	msg	
	PST ^	PST Files	pst	
	PST ANSI ^	PST Files	pst	
	TNEF Calendar Files **	EML Files	eml	
	TNEF File **	EML Files	eml	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
Microsoft Office	Excel	Microsoft Office	xls	xlt, xml
	Excel (2007-2010)	Microsoft Office	xlsx	
	Excel on xml format ^	Malformed Microsoft Office	xls	
	Excel Template	Microsoft Office	xltx	
	Excel with Macros	Microsoft Office with Macros	xlsm	
	ExcelXML	Microsoft Office	xml	
	Internal Office XML ^	Text Files	xml	xml.rels, rels, vml
	Macro File ^	Office Macro Files	bin	
	Obsolete Office Files ** ^	Microsoft Office	wri	
	Power Point	Microsoft Office	ppt	pps, xml, pot
	Power Point (2007-2010)	Microsoft Office	pptx	ppsx, potx
	Power Point Slide (2007-2010)	Microsoft Office	sldx	
	Power Point Slide With Macros (2007-2010)	Microsoft Office with Macros	sldm	
	Power Point Template	Microsoft Office	potx	
	Power Point With Macros	Microsoft Office with Macros	pptm	
	PowerPointXML ^	Microsoft Office	xml	
	Printer Settings	Microsoft Office Embedded Files	bin	
	Project ^	Microsoft Office	mpp	mpx
	Visio ^	Microsoft Office	vsd	vss, bin
	Visio (2007-2010)	Microsoft Office	vsdx	
	Visio with Macros	Microsoft Office with Macros	vsdm	
	Word	Microsoft Office	doc	
	Word (2007-2010)	Microsoft Office	docx	dochtml
	Word Pre-2007 Template	Microsoft Office	dot	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
Microsoft Office (continued)	Word Template	Microsoft Office	dotx	
	Word with Macros	Microsoft Office with Macros	docm	dotm
	WordXML	Microsoft Office	xml	
Text	Text ^	Text Files	txt	delivery-status, disposition-notification, rfc822-headers, project, csv, cfg, chm, tsv, xsl, xml, xsd, bin, ini, log, xml.rels, vml, rels, doc, manifest, usp, h, abc123
	Postscript File ^	Text Files	ps	
	XML ^	Text Files	xml	
Ole **Note** This is an internal category. It does not appear for users to configure settings.	Bmp Ole Object	OLE Object	bin	
	Docm Ole Object	OLE Object	bin	
	Docx Ole Object	OLE Object	bin	
	Dotx Ole Object	OLE Object	bin	
	Pdf Ole Object	OLE Object	bin	
	Pptm Ole Object	OLE Object	bin	
	Pptx Ole Object	OLE Object	bin	
	Slide Ole Object	OLE Object	bin	
	SlideM Ole Object	OLE Object	bin	
	SlideX Ole Object	OLE Object	bin	
	Unknown Ole Object (see note)	OLE Object	bin	
	Xls Ole Object	OLE Object	xls	
	Xlsx Ole Object	OLE Object	bin	
Other	ACIS Solid Model File ^	CAD Files	sat	
	Adobe Air ** ^	Adobe	air	
	Binary Excel (2007-2010) ^	Microsoft Binary Office Files	xlsb	
	CATIA Product Data File ^	CAD Files	stp	step
	CD Audio Track Shortcut File ** ^	Media Files	cda	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	CSS ^	CSS	css	
	DB Files ^	Database Files	dbf	npa, dbt, wnd, tab, mdb
	Dicom File ^	Dicom Files	dcm	
	eDrawings File ^	CAD Files	easm	
	Embedded Macro Files ^	Embedded File	bin	
	Empty File ^	None		
	Equation Ole Object ^	OLE Object	bin	
	Excel95 File ^	Unsupported Files	xls	
	HTML ^	HTML Files	html	htm
	HTML Attachments ^	HTML Files	html	htm
	HWP 3.0 File ^	Hancom Files	hwp	
	INF File ^	INF Files	inf	
	Initial Graphics Specification File ^	CAD Files	igs	
	IPC files ** ^	FORTRAN program File	ipc	
	JAR ^	JAR Files	jar	jarxx
	LabView ** ^	LabView	vi	
	Material Exchange Format File ** ^	Media Files	mxf	
	Media File ^	Media Files	mp3	wav, wmv, ico, mpg, mpeg, flv, wma, avi, mp2, mp4, m4a, 3gp, mts, mkv, vob
	MHT File ^	MHT Files	mht	
	MST files ** ^	Installer Setup File	mst	
	p7s ^	Digital Signatures	p7s	
	Parasolid model File ** ^	CAD Files	x_t	x_b
	Pcx File ^	CAD Files	pcx	
	Pgp File ^	Encrypted Files	pgp	
	PowerPoint95 File ^	Unsupported Files	ppt	
	PreR14Dwg File ^	CAD Files	dwg	
	PreWord97 File ^	Unsupported Files	doc	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	PSD File ^	Photoshop Files	psd	
	RPT ** ^	RPT Files	rpt	
	RSP File ** ^	PLC Files	rsp	
	Script ^	Batch Files	bat	js, php, cmd, vbs, reg, pl, lnk, py, asp
	Shortcut File ^	Shortcut Files	url	
	SolidWorks File ^	CAD Files	sldasm	sldprt
	Solution User Option File ** ^	Visual Studio Files	suo	
	SQL File ** ^	SQL Files	sql	
	Statistical Files ** ^	Statistical Files	dta	sas7bdat
	Thumbnail File ^	Thumbnail Database Files	db	
	Unrecognized ^	Any Binary Files		
	VCF ^	Exchange	vcf	
	XFA ^	Xfa Files	pdf	
	XDW ^	DocuWorks Files	xdw	
	ZSoft PCX Bitmap File ^	CAD Files	brd	

Notes

- Unknown Ole Objects: Both generic and unknown Ole objects are handled.
- Generic Ole objects will be sanitized, and unknown Ole objects will be blocked.

2 Installing Votiro Disarmer

It is recommended to install Disarmer and the Management Platform on different servers. If you choose, however, to install them on the same server, ensure that you install Disarmer **before** you install the Management Platform. Instructions for installing the Votiro Management Platform are provided in Installing Votiro Management Platform on page 26.

Use the setup wizard to install the Disarmer. The wizard verifies that the prerequisite software is installed, then, assuming an internet connection exists, installs any components that are missing.

Notes

- It is recommended that a dedicated server, without any add-ons or tools, be used for the Disarmer installation.
- The recommended hardware requirements are based on the projected load and file traffic volume.

When the installation is completed, a message, indicating that Disarmer has been successfully installed, is displayed.

Following installation, it is recommended you perform various post-installation steps. For more information, see Post-Installation Steps on page 20.

2.1 Requirements

2.1.1 Hardware Requirements

The following requirements are the minimum and recommended hardware requirements for running Disarmer version 8.4. The minimum requirements are not recommended for production environments.

Table 2 Disarmer Hardware Requirements

Required Item	Minimum	Recommended	Comment
CPU	One 2.66 GHz CPU	Quad Core 2.66 GHz CPU	Number of cores is determined by the requested volume of traffic. Can be vCPU on a virtual machine.
RAM	At least 16 GB of RAM	At least 32 GB of RAM	
Operating system drive	At least 30 GB of free space		Can be a virtual hard disk.
Workspace drive	At least 100 GB of free space		SSD or other fast storage is recommended.

Required Item	Minimum	Recommended	Comment
Network Card			Can be a virtual network card (vNIC) on a virtual machine.

Note

The recommended requirements are based on the projected load and email traffic. The metrics vary from organization to organization.

2.1.2 Software Requirements

Operating System

The following software must be pre-installed and configured before you run the Disarmer setup wizard:

- Microsoft Windows Server 2012 R2, with the latest rollups and updates installed, or Microsoft Windows Server 2016 with the latest updates installed.
- The default language for non-Unicode programs is set to your preferred language under the **Region** > **Administrative** tab.

Software

The following software is downloaded by the installer:

- Microsoft .NET Framework 4.6.1
- Microsoft Message Queuing
- Microsoft Visual C++ Redistributable Package for Visual Studio 2010: 64-bit
- Microsoft Visual C++ Redistributable Packages for Visual Studio 2013: 64-bit
- Microsoft Visual C++ Redistributable Packages for Visual Studio 2015: 32-bit

2.1.3 Network Requirements

Table 3 Disarmer Firewall Rules

Source Host	Source Port	Destination Host	Destination Port
User Application	Any	Disarmer	TCP 80 TCP 443
Disarmer	Any	Internet (Any)	TCP 80 TCP 443
Management	Any	Disarmer	TCP 80 TCP 443

Load Balancing and High Availability

Disarmer supports load balancing and high availability. This can be achieved by using either of these two options:

- An application delivery controller.
- A Layer 7 load balancer that supports sticky-session and HTTP cookie-based load balancing.

2.1.4 Internet Connectivity

Disarmer requires an internet connection for downloading the prerequisite software and for updates of definition files from antivirus vendors' servers.

Disarmer does not require an internet connection to run the sanitization engine.

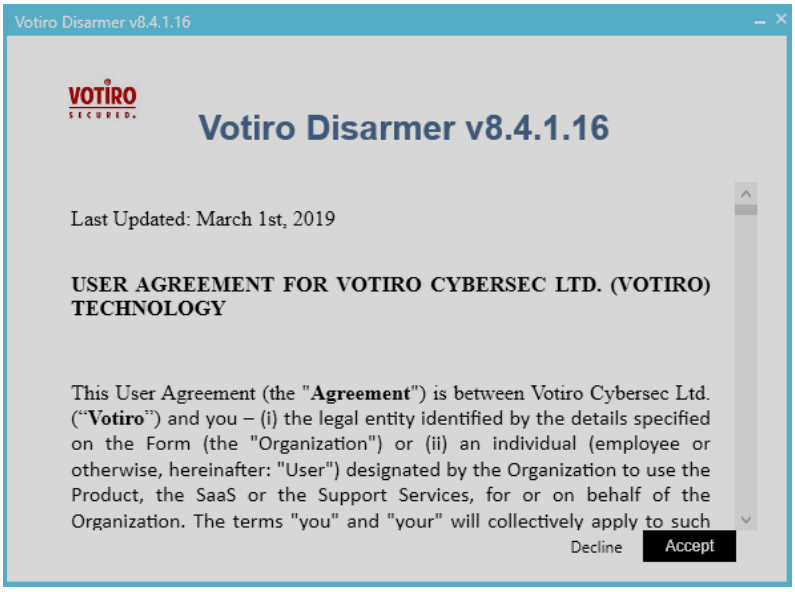
2.2 Running the Installation

You must have administrator privileges on the computer to install Votiro Disamer.

Be aware that the Disarmer setup installs several Windows Services. They are listed in Windows Services Installed with Votiro Products on page 111.

> **Note**
> Before running the installation, turn off any third-party antivirus software that is running on the target system.

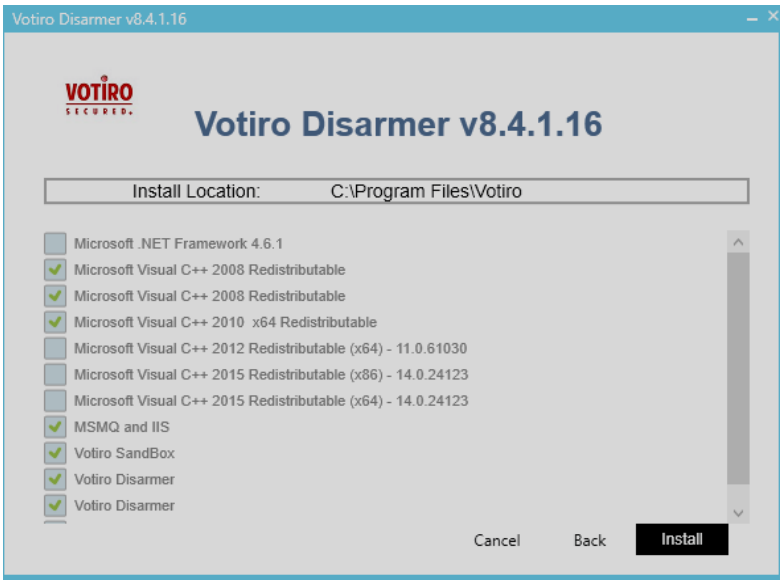
1. Run the Disarmer setup.



2. Click **Accept** to accept the terms of use.

3. The default path for the installation is shown. Accept the default location, or choose another location.

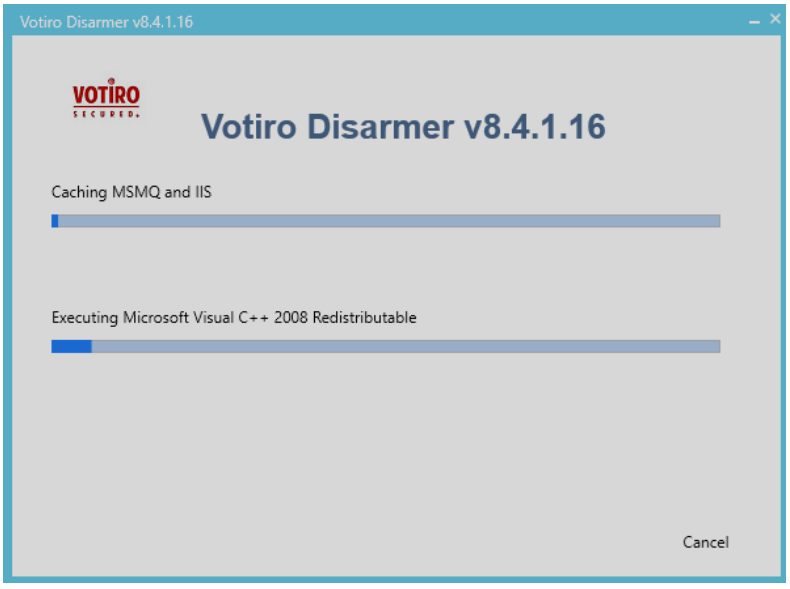
4. Click **Next** to display the list of prerequisites.



The installer checks the items that were not identified in your system. These items will be downloaded as part of the installation.

5. Click **Install** to proceed.

The installation begins. The setup progress screen is displayed during the installation process.



6. When the notification *Votiro Disarmer is ready for use* is displayed, click **Close**.

> **Note**
> The first update of the antivirus engine begins after installation. This might take several minutes. Sanitization is disabled during this update process.

2.3 Post-Installation Steps

After you have completed the Votiro Disarmer installation, verify that it was successful and obtain a license key.

2.3.1 Obtaining a License Key

To obtain a permanent Votiro Disarmer license key you must perform the following steps:

1. Create a MachineStats.xml file.
2. Send the MachineStats.xml file to Votiro Support.
3. Receive a license file from Votiro Support.
4. Save to license file in the appropriate folder.

The MachineStats.xml file contains information on the machine that Votiro Disarmer is installed on, such as OS version, memory size and number of cores.

Votiro Support generate a corresponding license key for Votiro Disarmer, which is required for product activation.

Procedure

1. Using the link you received from Votiro Support, download the MachineStats.zip file to the Votiro Disarmer server.
2. Extract the zip file.
3. Open CMD with Administrator privileges.
4. Navigate to the MachineStats folder.
5. Run the following command:

   ```
   MachineKeyTool.exe -o c:\
   [FullFileOutputPath]\MachineStats.xml
   ```

   A MachineStats.xml file is created in the chosen destination folder.
6. Send the MachineStats.xml file to Votiro Support via email or via Votiro's Customer Portal.

   Votiro Support will provide a license file (VotiroLicense.xml).
7. Place the license file in the SDS-WS installation root folder. The default location is:

C:\Program Files\Votiro\SDS Web Service.

Verifying Votiro Disarmer Activation

To verify that Votiro Disarmer has been successfully activated, navigate to the API log file (the default location is: C:\Program Files\Votiro\SDS Web Service\Logs\API).

The following is an example of output that should appear in the log:

```
4880-1 | 17/07/2018 16:16:00.208 | 2 Info | License was
validated successfully, license details.
```

> **Note**
> It can take up to 30 minutes for the information to appear in the API log.

Renewing Your Votiro License Key

To renew your license key contact Votiro Support for a replacement VotiroLicense.xml file. Provide a new MachineStats.xml file if the OS version, memory size or number of cores in your environment have changed since receiving the last VotiroLicense.xml file.

> **WARNING!**
> Replace your license key when renewal is required. Votiro will continue running for a grace period after the renewal date, providing time for you to receive and install the new license key.

At the expiration of the grace period Votiro Disarmer services are stopped and files will not be sanitized.

2.3.2 Verifying that Votiro Windows Services Are Active and Running

The services described in the following table are installed as part of the Disarmer product:

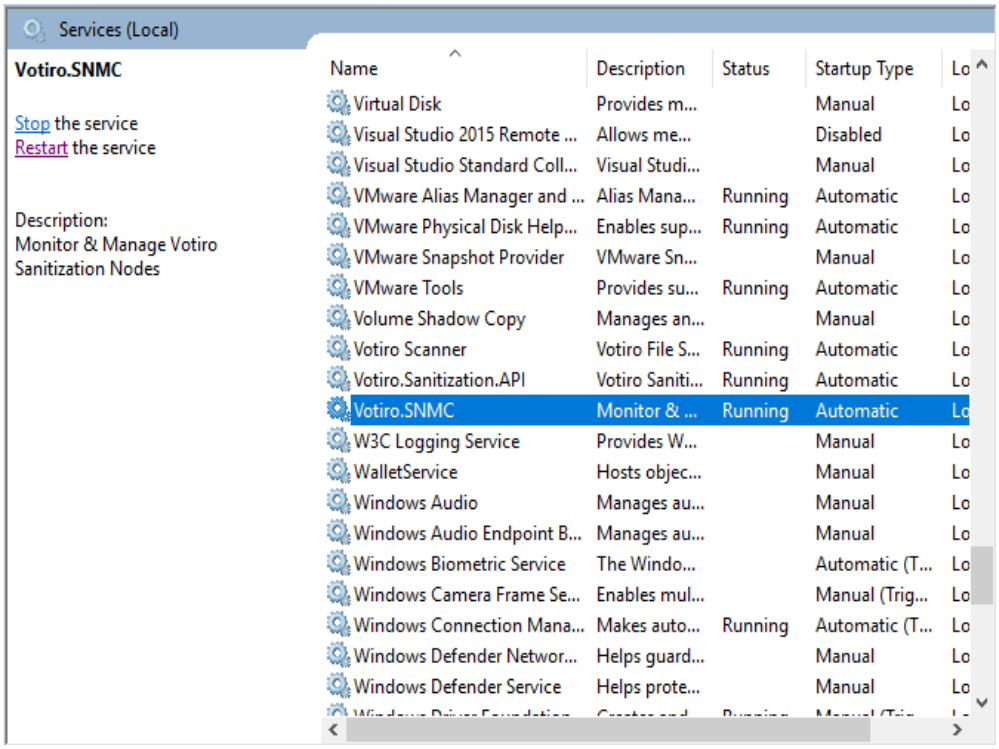
Table 4 Votiro Disarmer Windows Services and Log Locations

Service	Description
Votiro Scanner	The Votiro Scanner service is located at: *[installation_path]*\Votiro\Votiro.Malware.Scanner. The Votiro Scanner service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\Votiro.Malware.Scanner\Logs.

Service	Description
Votiro.Sanitization.API	The Votiro.Sanitization.API service is located at: [*instalation_path*]\Votiro\SDS Web Service. The Votiro.Sanitization.API service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\SDS Web Service\Logs\API.
Votiro.SNMC	The Votiro.SNMC service is located at: [*installation_path*]\Votiro\SDS Web Service. The Votiro.SNMC service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\SDS Web Service\Logs\SNMC. The SNMC manages *n* sanitization nodes. Nodes have log files that are located at: [*installation_path*]\Votiro\Logs\SNMC\1 ... *n*
Votiro.Sandbox	The Votiro.Sandbox service is located at: [*instalation_path*]\Votiro\Sandbox. The Votiro.Sandbox service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\Sandbox\Logs.

To check that these services are all active and running:

1. Navigate to the Windows Services screen: **Windows** > **Administrative Tools** > **Services**.
2. Locate the Votiro Disarmer Windows Services that are detailed in the table above:
   - Votiro Scanner
   - Votiro.Sanitization.API
   - Votiro.SNMC
   - Votiro.Sandbox



3. For each of these services, ensure that the following details are displayed:
   - Status is Running.
   - Startup Type is Automatic.

The Votiro Scanner service is dependent on the MS Windows Net.Pipe Listener Adapter service. Check that the status of the Votiro Scanner service is Running.

2.3.3 Enabling HTTPS (SSL) on the Votiro.Sanitization.API Service

An SSL certificate is used to establish a secure encrypted connection between a browser and a server. An SSL certificate must be installed on the server and all browsers that connect to the Disarmer using HTTPS.

You must have administrator privileges on the server hosting Disarmer and access to the Windows SDK to use the file makecert.exe.

The procedure includes generating and installing an SSL certificate. If you already have an SSL certificate, skip to step 2.

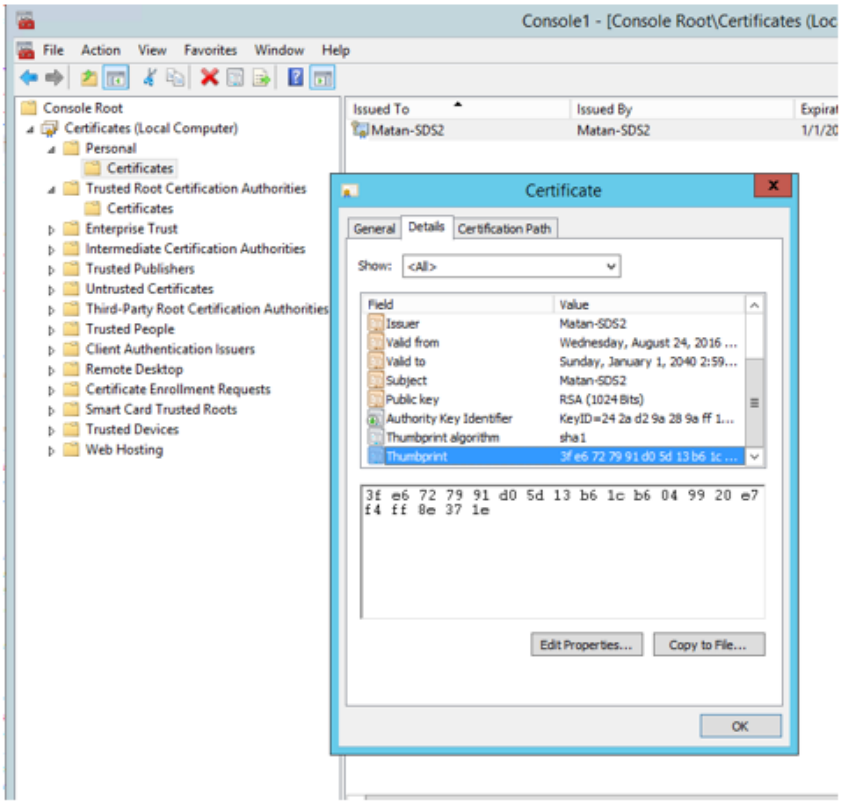
Procedure:

1. Create and install a certificate on the server that hosts Disarmer:

a. Create a ROOT certificate by issuing the following command: makecert.exe -sk RootCA -sky signature -pe -n CN= [MachineHostName] -r -sr LocalMachine -ss Root [RootCertName].cer

b. Create a server certificate: makecert.exe -sk server -sky exchange -pe -n CN=[MachineHostName] -ir LocalMachine -is Root -ic [RootCertName].cer -sr LocalMachine -ss My [CertName].cer

c. Browse to the Windows Certificate list and verify that a new valid certificate exists under the Personal path.



d. The **Certificate Path** should contain two levels with Certificate Status stating *This certificate is OK*.

e. Copy the server certificate's Thumbprint under **Details** > **Thumbprint**.

> **Note**
> Remove all spaces from the Thumbprint before copying.

f. Bind the server certificate to your SSL port (default: 443) with the following command:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=
[thumbprint] appid={b6445322-3509-4d0f-8b4b-0a12eeadaed0}
```

2. Restart the Votiro.Sanitization.API and Votiro.SNMC Windows services.

3. Browse to https://[MachineHostName]/SdsService/v3, replacing [*MachineHostName*] with the server host. Verify that there is no certificate warning or validation issue. You should expect the *Endpoint not found* message.

> **Note**
>
> Your API client might enforce a valid certificate. In such a case, the Root certificate ([*RootCertName*].cer) generated in step 1 must be installed in the local certificate store.

3 Installing Votiro Management Platform

Votiro's Management Platform performs two main functions:

- Provides a dashboard for:
  - Viewing and editing Disarmer's sanitization policies.
  - Displaying data and statistics about the sanitized files.
  - Managing incidents.
- Stores original and sanitized files using encryption. The files are used for analysis and zero-day identifier purposes.

This chapter describes the procedures to perform when installing Votiro Management Platform for the first time.

Installing the Management Platform is performed using a setup wizard. The wizard verifies that the prerequisite software is installed and, assuming an internet connection exists, installs any components that are missing.

Notes

- It is recommended that a dedicated server without any add-ons or tools be used for the Management Platform installation.
- Disarmer and the Management Platform must be installed on different servers, particularly in production environments.

3.1 Requirements

3.1.1 Hardware Requirements

The following requirements are the minimum and recommended hardware requirements for running Management version 8.4. The minimum requirements are not recommended for production environments.

Table 5 Management Hardware Requirements

Required Item	Minimum	Recommended	Comment
CPU	Two Core 2.66 GHz CPU	Quad Core 2.66 GHz CPU	The number of cores is determined by the requested volume of traffic. The CPU can be a vCPU on a virtual machine.

Required Item	Minimum	Recommended	Comment
RAM	At least 8 GB of RAM	At least 16 GB of RAM	For optimizing ElasticSearch (ES), which is used in Management, the following recommendations should be followed: ■ The ES heap should be assigned 50% of the hosting machine RAM. The other 50% should be left free for the operating system. ■ The maximum heap size to allocate, even if more RAM is available, is 32 GB. ■ A heap size smaller than 4 GB is strongly discouraged. ■ The bootstrap.memory_lock flag should always be on. The Management installer activates the bootstrap.memory_lock flag and sets the appropriate heap size.
Operating system drive	At least 100 GB of free space	At least 100 GB of free space	Can be a virtual hard disk.
Blob Storage drive	At least 100 GB of free space	At least 500 GB of free space	SSD or other fast storage is recommended. Note The file system must be formatted as NTFS.

Note

The recommended requirements are based on the projected load and email traffic. The metrics vary from organization to organization.

3.1.2 Software Requirements

Operating System

The following software must be pre-installed and configured before you run the Management Platform setup wizard:

- Microsoft Windows Server 2012 R2, with the latest rollups and updates installed, or Microsoft Windows Server 2016, with the latest updates installed.
- The default language for non-Unicode programs is set to your preferred language under the **Region** > **Administrative** tab.

- Oracle JDK or OpenJDK version 1.8.0.242. For additional information about installing OpenJDK, see the article Votiro Management Using OpenJDK in the Votiro Help Center.

Public Key Policies - Encrypting File System

Votiro Disarmer requires the Encrypting File System to have a valid certificate with an expiration date in the future.

Check the certificate in the Encrypting File System. To locate the file:

1. Navigate to the **Group Policy** tab.
2. **Click** <*Default Domain Policy GPO*>, then select **Edit**.
3. Navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Encrypting File System**.
4. Ensure a certificate is present with an expiration date in the future.

Software

Provided you have an Internet connection, the installation wizard checks that the required components are present in the target system and downloads any that are missing.

3.1.3 Network Requirements

Table 6 Management Firewall Rules

Source Host	Source Port	Destination Host	Destination Port
Disarmer	Any	Management	TCP 3030 TCP 7070
Management	Any	Internet (Any)	TCP 80 TCP 443

Load Balancing and High Availability

Disarmer supports load balancing and high availability. This can be achieved by using either of these two options:

- An application delivery controller.
- A Layer 7 load balancer that supports sticky-session and HTTP cookie-based load balancing.

3.1.4 Internet Connectivity

An internt connection is required for properly installing and operating theVotiro Management Platform.

The connection is required for downloading prerequisite software, updating the antivirus engine, running the Votiro URL reputation service, and identifying zero-day attacks.

3.2 Running the Votiro Management Platform Installation

You must have administrator privileges on the computer to install the Management Platform.

Be aware that the Management Platform setup installs several Windows Services. They are listed in Windows Services Installed with Votiro Products on page 111.

> **Note**
> Before running the installation, turn off any third-party antivirus software that is running on the target system.

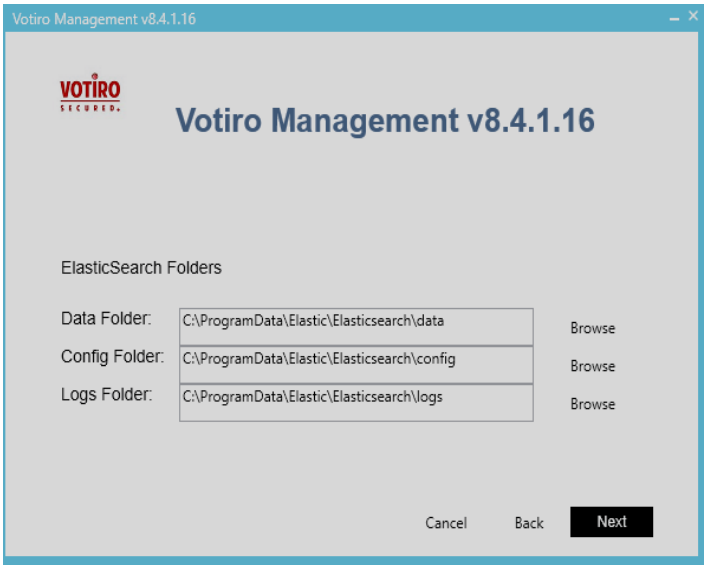
1. Run the Management Setup.

2. Click **Accept** to accept the terms of use.

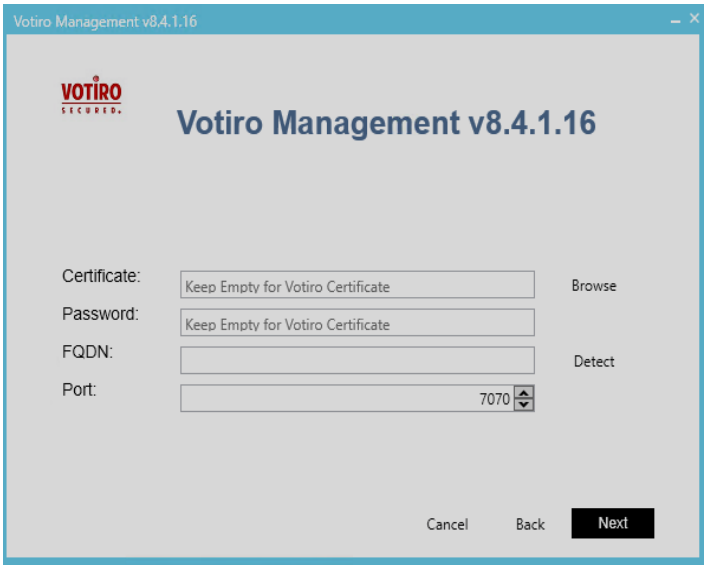
   The following window is displayed:

3. Accept the default location, C:\Program Files\Votiro, or choose a different location. Click **Next**.

   The following window is displayed:



4. Accept the default locations for ElasticSearch data, configuration, and logs folders. Click **Next**.



5. Select a certificate authority. Either accept the default Votiro setting, or specify your organization's SSL certificate authority, together with the password.

6. Accept the default port, 7070, or specify a different port. Click **Next**.

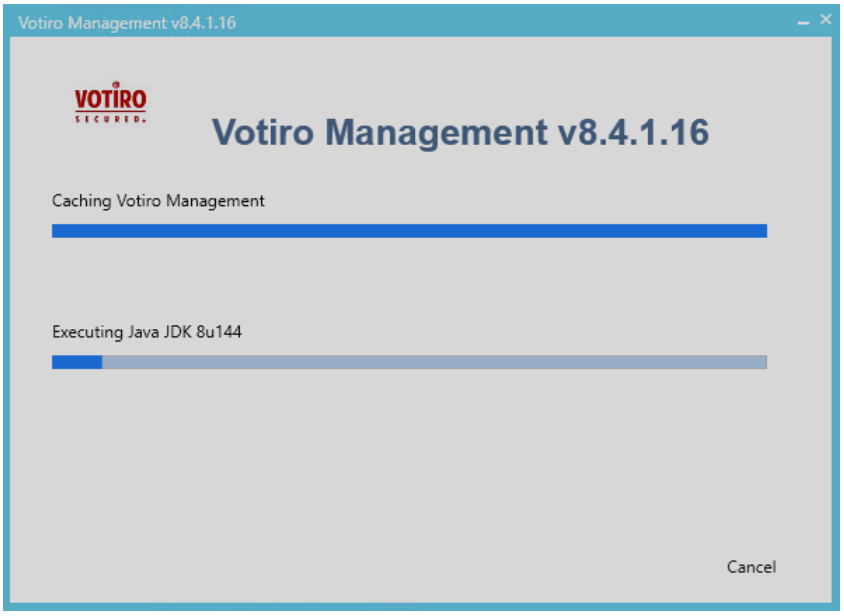
   The following window is displayed:

- The location for installation, certificate, password, and port number that have been specified so far are displayed. Click **Back** if you want to review them.

- The installer checks the items that were not identified in your system. These items will be downloaded as part of the installation. Click **Install** to proceed.

7. Click **Install**.

   The installation begins. The setup progress screen is displayed during the installation process.



   When the installation is completed, the notification "**Votiro Management is ready for use**" is displayed.

8. Click **Close**.

> **Note**
>
> Following the successful installation of the Management Platform, it is highly recommended that you modify the default location of the the blob storage. See Storage folder on page 72.

3.3 Post-Installation Steps

After you have completed the Votiro Management Platform installation, verify that it was successful.

The services described in Votiro Management Platform Windows Services and Log Locations on the next page are installed as part of the Management Platform:

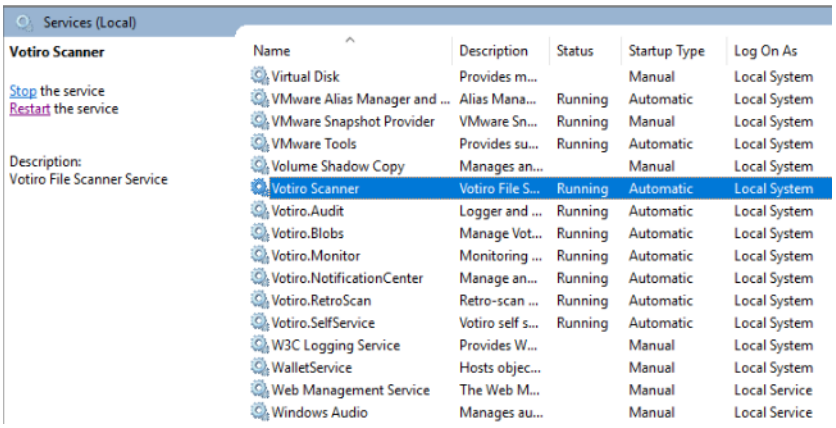
Table 7 Votiro Management Platform Windows Services and Log Locations

Service	Description
Votiro.Blobs	The Votiro.Blobs service is located at: *[installation_path]*\Votiro\BlobStorage. The Votiro.Blobs service maintains a log file for all activity. The log file is located at: *[installation_path]*\Votiro\BlobStorage\Logs.
Votiro.NotificationCenter	The Votiro.NotificationCenter service is located at: [*installation_path*]\Votiro\NotificationCenter. The Votiro.NotificationCenter service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\NotificationCenter\Logs.
Votiro.RetroScan	The Votiro.RetroScan service is located at: [*installation_path*]\Votiro\RetroScan. The Votiro.RetroScan service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\RetroScan\Logs.
Votiro Scanner	The Votiro Scanner service is located at: *[installation_path]*\Votiro\Votiro.Malware.Scanner. The Votiro Scanner service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\ Votiro.Malware.Scanner\Logs.
Votiro.Audit	The Votiro.Audit service is located at: [*installation_path*]\Votiro\Audit. The Votiro.Audit service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\Audit\Logs.
Votiro.Monitor	The Votiro.Monitor service is located at: [*installation_path*]\Votiro\Monitor. The Votiro.Monitor service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\Monitor\Logs.
Votiro.SelfService	The Votiro.SelfService is located at: [*installation_path*]\Votiro\PpfSelfService. The Votiro.SelfService service maintains a log file for all activity. The log file is located at: [*installation_path*]\Votiro\PpfSelfService\Logs.

Service	Description
Elasticsearch	The Elasticsearch service is located at: C:\Program Files\Elastic\ElasticSearch. The Elasticsearch service maintains a log file for all activity. The log file is located at: C:\ProgramData\Elastic\Elasticsearch\logs.

To check that these services are all active and running:

1. Navigate to the Windows Services screen: **Windows** > **Administrative Tools** > **Services**.
2. Locate the Votiro Management Platform Windows Services that are detailed in the table above:



3. For each of these services, ensure that the following details are displayed:
   - Status is Running.
   - Startup Type is Automatic.

4 Configuring Votiro Disarmer

This chapter describes the configurations you must perform so that the Disarmer engine and Management Platform work together.

Antivirus Settings

To prevent any failures that may occur if Votiro application files are scanned, before configuring Votiro Disarmer, perform the following action in both the Windows Servers that are hosting the Disarmer engine and the Management Platform:

> **Note**
> Make sure to turn on the antivirus, as it was turned off prior to installation.

In your antivirus settings, add the following exclusions:

- Votiro Disarmer installation files in the folder [*installation_path*]\Votiro.
- Votiro Disarmer Windows temporary folder c:\Windows\Temp.
- Votiro Management blob folder. The default location is c:\blobStorage. For more information, see Storage folder on page 72.

4.1 Adding Authentication Tokens for Policy Updates

Provide authorization tokens to be used in requests from the Disarmer engine for Policy updates in the Management Platform.

Open the webapi.xml configuration file that is located in [*installation_path*]\Votiro\SDS Web Service\config.

Edit <WebApiServerConfig> as follows:

1. Ensure that NamedPolicyFolderPath is set to "" (empty).
2. Point NamedPolicyServerUri to the Management server. Use the syntax: https://[*hostname*]:[*portnumber*], where *hostname* represents a fully qualified hostname.
3. Ensure that the AuthToken is set to the same value specified for <AuthorizedTokens> and <ClientToken> in <appSettings> of the configuration files in the Management platform.
4. Ensure that the UnknownPolicyHandling is set to "Block" or "Reject".
   - When set to "Block" the request is processed, then blocked.
   - When set to "Reject" the API does not process the request.
5. Ensure that an UnknownPolicyBlockMessage is defined (use the default message or create a customized message).
6. Set the NamedPolicyServerUri to "https://my_management_server:7070".

Example

```
<WebApiServerConfig

  NamedPolicyFolderPath=""

  NamedPolicyServerUri="https://my_management_
server:7070"

  AuthToken="30acc6eb-16d9-4133-ae43-0f5b6d40a318"

  UnknownPolicyHandling="Block"

  UnknownPolicyBlockMessage="File was blocked due to
an error in Policy process. Please contact your system
administrator."/>
```

4.1.1 Editing API Authorization Token

To enable and edit the API Authorization Token:

1. Open the webapi.xml configuration file that is located in [*installation_path*]\Votiro\SDS Web Service\config.
2. Add SdsApiToken = <yourToken>.
3. Configure your connector:
   a. Reference client: -key <yourToken>.
   b. File Connector / Email Conector: update CloudApiKey parameter with the generated token.
   c. With PostMan: add “Ocp-Apim-Subscription-Key” header key and the generated token as the value.

4.2 Configuring Publish Action

Add a policy action that instructs the Disarmer engine to publish sanitization activity to the Management Platform.

Open the publish.xml configuration file that is located in [*installation_path*]\Votiro\SDS Web Service\Policy.

Add a definition for <PolicyAction>. For type, specify ReportToManagementAction.

Example

```
<PolicyRule>

<Filter xsi:type="NoFilter" />

<Actions>

<PolicyAction xsi:type="ReportToManagementAction"/>
```

```
</Actions>

</PolicyRule>
```

4.3 Configuring the Management Platform

Use the machine.xml file to configure settings related to the Votiro Management Platform.

The machine.xml file is located in [*installation_path*]\Votiro\SDS Web Service\config.

Table 8 Management Platform Configuration File Attributes

Attribute	Description	Value
ManagementSettings		
SanitizationInfoServerUrl	Specifies the location of the Votiro Management server to which sanitization metadata must be published.	Specify the location in the format: https://[*hostname*]:[*portnumber*] where *hostname* represents a fully qualified hostname. By default, *portnumber* is 7070.
BlobManagerServerUrl	Specifies the location of the Votiro Management server on which original and sanitized files are stored.	Specify the location in the format: https://[*hostname*]:3030, where *hostname* represents a fully qualified hostname or an Ipv4 address.
AuthToken	Defines the authentication tokens that will be recognized by Disarmer during the process of publishing to the Votiro Management server.	This value must be identical to that specified for AuthToken in the webapi.xml configuration file. The value you specify must be a string that uses Latin and alphanumeric characters only.
RequestTimeoutInSeconds	Defines the maximum amount of time within which to attempt to write a file to the blob.	The default is 60 seconds.

> **Note**
> The AuthToken value must be identical to the setting in the webapi.xml configuration file. See Adding Authentication Tokens for Policy Updates on page 35. In addition, review settings for AuthorizedTokens and ClientToken in the configuration files, see Authentication Tokens on page 40.

4.4 Installing the Management Certificate in Disarmer Servers

You must ensure that the certificate that is installed in the Disarmer server is the same as that installed in the Management Platform server.

- If you are using the Votiro certificate that is provided with the Management Platform installation, follow the procedures in this section.
- If you are using a company certificate, ensure that it is installed under Trusted Root Certificate Authority in every Disarmer server that must communicate with Management.

To export the certificate from the management platform:

1. In the server that is hosting the Management Platform, launch the Certificate Manager tool.
2. Click **Trusted Root Certificate Authorities** > **Certificates**.
3. Locate the Votiro Management certificate (it appears in the Friendly Name column as "Votiro_wixCert_1"). Right-click it, then select **All Tasks > Export.**
4. In the **Certificate Export Wizard** that appears, click **Next**. Click **Next** until you are prompted for the location and name of the certificate that you are going to export.
5. Browse to the target folder.
6. Enter a name for the certificate to export. Click **Save**.
7. Copy the certificate to the Clipboard.

To import the certificate to a Disarmer server:

1. Paste the certificate from the clipboard into the computer that is hosting the Disarmer engine.
2. Double-click the certificate.
3. In the **Certificate** dialog that appears, click **Install Certificate**.
4. Select **Local Machine** and click **Next**.
5. In the **Certificate Store**, select **Place all certificates in the following store**.
6. Browse to **Trusted Root Certificate Authorities** and click **OK**.
7. Click **Next**.

8. Click **Finish**.

Repeat steps 1 - 8 for all Disarmer servers that must communicate with the Management Platform.

4.5 Optional Configurations

The following settings can be configured for customizing the Disarmer Engine to your organization's requirements:

- Publishing and Storage Settings
- Authentication Tokens
- Machine Settings
- Votiro Disarmer API Settings
- Sanitization API Settings
- Sanitization Node Monitor Controller (SNMC) Settings
- Sanitization Node Settings
- Scanner (Antivirus) Settings
- SIEM Report Settings
- Logs Settings
- Active Directory
- Configuring for Policy by Active Directory
- Sandbox Settings

In all files, default configuration values are already specified; modify them as needed. Exercise caution when changing configuration values. Some settings affect performance and might increase the time that it takes to process each file. In the description of each of the configuration files, attributes that affect performance are identified or marked with Caution.

Updating Configuration Files

To change configuration values, open the XML file in an XML or text editor.

After you have made your changes and saved the file, you must restart the following services to initiate the changes:

- **For Scanner settings**: restart the Votiro Scanner Windows service.
- **For Sandbox settings**: restart the Votiro.Sandbox Windows service.
- **For all other configuration files**: restart the Votiro.Sanitization.API and Votiro.SNMC Windows services. In addition, run the iisreset command using administration privileges.

AppenderConfig LogLevel settings take effect immediately, without service restart.

You can edit and save more than one configuration file before restarting the services.

4.5.1 Publishing and Storage Settings

Select the Management server on which you want to publish and store sanitization data. For publishing and storage, ensure you have configured the following settings in the machine.xml file:

- SanitizationInfoServerUrl.
- BlobManagerServerUrl.
- AuthToken.

> **Note**
> It is recommended to specify the same Management server for all three attributes.

For further details on the file attribute configuration settings, see Configuring the Management Platform on page 37.

When the changes have been applied, ensure that you:

1. Restart the Votiro.Sanitization.API and Votiro.SNMC Windows services.
2. Run the iisreset command using administration privileges.

Example

The following example demonstrates the three settings described in this section:

```
<VotiroConfiguration>

<MachineSettings>

...

  <ManagementSettings
   SanitizationInfoServerUrl= "https://my_
  management_server:7070"
   BlobManagerServerUrl= "http://my_management_
  server:3030" AuthToken="30acc6eb-16d9-4133-ae43-
  0f5b6d40a318"/>

  </MachineSettings>

</VotiroConfiguration>
```

4.5.2 Authentication Tokens

Perform the instructions provided in this section in all of the following configuration files:

- Management.BlobStorage.WindowsService.exe.config, under [*installation path*]\Votiro\BlobStorage
- Management.NotificationCenter.WindowsService.exe.config, under [*installation path*]\Votiro\NotificationCenter
- Management.RetroScan.WindowsService.exe.config, under [*installation path*]\Votiro\RetroScan
- web.config, under [*installation path*]\Votiro\Management
- Management.Audit.WindowsService.exe.config under [*installation path*]\Votiro\Audit
- Management.Monitor.WindowsService.exe.config under [*installation path*]\Votiro\Monitor
- Management.SelfService.WindowsService.exe.config under [*installation path*]\PpfSelfService

1. Open each configuration file.
2. In each, add keys under <appSettings> for <ClientToken> and <AuthorizedTokens>.

Example

```
<appSettings>

  . . .

  <add key="ClientToken" value="30acc6eb-16d9-4133-ae43-
  0f5b6d40a318"/>

  <add key="AuthorizedTokens" value="30acc6eb-16d9-4133-ae43-
  0f5b6d40a318"/>

</appSettings>
```

> **Note**
> The values for <AuthorizedTokens> and <ClientToken> must be identical. They must also be identical to the value of <AuthToken> in the webapi.xml configuration file.

3. Save the files.
4. For changes to take effect, ensure that you:
   a. Restart the Votiro.Blobs, Votiro.NotificationCenter, Votiro.RetroScan, Votiro.Audit, Votiro.Monitor, and Votiro.SelfService Windows services.
   b. Run the iisreset command using administration privileges.

4.5.3 Machine Settings

Use the machine.xml file to define settings related to the system name, policies, and general system parameters.

The machine.xml file is located in:

[*installation_path*]\Votiro\SDS Web Service\config.

The attributes described in Table 9 Machine Settings Configuration File Attributes appear in the machine.xml file. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

In addition, you must specify the update interval value and other attributes for each antivirus engine.

Table 9 Machine Settings Configuration File Attributes

Attribute	Description	Value
GeneralSettings		
SystemName	Specifies the name of the Votiro system on a specific machine. The system name defines the source of the information, which is important when you have more than one machine in your environment that you might need to identify for logging and notification purposes.	A string that uniquely identifies the system on the specific machine. The default is Votiro Zero-Day Exploit Protection.
PolicySettings		
PolicyFileName	Specifies the name of the sanitization policy. This is the filename only, without the file extension of the policy file under the PolicyFolder. The default path is [installation_path]\Policy.	Changing the default from sanitize_webserv is not recommended.

Attribute	Description	Value
BlockedFileType	Specifies whether a blocked file will be replaced by a PDF or TXT file following sanitization. For example, a malicious email attachment letter.doc, which must be blocked will be replaced with either letter_blocked.pdf or letter_blocked.txt, depending on this setting. The content of the PDF or TXT file describes the reason of blocking and basic information.	A file type, either PDF or TXT. Default is PDF.
BlockedFileTemplate	Specifies the path to the template file used to create a replacement email after blocking by sanitization.	If the file to be replaced is a PDF type file, the path should point to an RTF file. If the file to be replaced is a TXT type file, the path should point to a TXT file. Default is [*installation_path*]\Templates\Blocked\blocked.rtf
BlockedFileDictionary	Specifies the path to the dictionary file used to create a replacement email after blocking by sanitization.	Default is [*installation_path*]\Templates\Dictionaries\blocked.xml
SystemSettings		
PolicyFolder	Specifies the name of the policies folder for global sanitization and publish policies.	Do not change the default. Leave empty to specify the default %HomeDirectory%\Policy.
TempFolder	Specifies the path and name of the temporary workspace folder. Use the absolute path to the folder.	You do not need to specify a value for this attribute.

Attribute	Description	Value
MaxTempFileAgeInMin	Specifies the general configuration for the TempFolder cleaner. This is the maximum amount of time in minutes that a temporary file exists before automatic deletion.	A positive integer representing the minutes. The default is 60. **Note** The value that you set affects performance and disk utilization.
MaxCpuUsagePercentageForDequeue	Specifies the maximum threshold of the CPU within which a sanitization job may start, expressed as a percentage. Before starting a new sanitization job, the service verifies that the CPU is not above the threshold. If it is above that threshold, the job is not queued until the CPU load drops below the specified percentage.	A positive integer between 1 and 100. The default is 90. **Note** The value that you set affects performance.
QueuePollingIntervalInMS	Specifies the length of time in milliseconds between two subsequent polls for queue availability.	A positive integer representing milliseconds. The default value is 100. **Note** The value that you set affects performance.
CloudVotiroSettings		
Enabled	Determines if the URL Reputation service is enabled or not. When enabled, the URL Reputation feature allows you to block access to web addresses identified as containing malicious content.	True to enable the service; False to disable the service. The default is False.

Attribute	Description	Value
Address	Specifies the address where the URL Reputation service is hosted. **Note** The service requires **Block files with suspicious links** to be checked. This option is available when defining policies by file types: PDF, Email, and Office.	Specify the location in the format: https://[*address*] For example, https://safeurl.prod.votiro.com.
CustomerId	Personalized customer ID.	Contact Votiro Support.
SelfServiceSettings		
UsersPortalAddress	Specifies the location of a Votiro Management server. The server hosts the web page in which a password is entered to release a blocked password-protected file.	Specify the location in the format: https://[*hostname*]:[*portnumber*] where *hostname* represents a fully qualified hostname. The default is the address specified for SanitizationInfoServerUrl, under <ManagementSettings>.
SandboxServiceSettings		
SandboxServiceAddress	Sandbox service address.	Specify the location in the format: https://[*hostname*]:[*portnumber*] where *hostname* represents a fully qualified hostname. The default is: "http://localhost:4318" Do not change this value unless instructed by Votiro Support.

4.5.4 Votiro Disarmer API Settings

Use the webapi.xml file to define attributes for the Votiro Disarmer API.

The Disarmer API configuration file is located in:

`[installation_path]\Votiro\SDS Web Service\Config.`

The attributes are described in Table 10 API Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 10 API Configuration File Attributes

Attribute	Description	Value
WebApiServerConfig		
NamedPolicyCacheInMin	Time during which the Disarmer server uses the cached policy. In the event that the Disarmer engine loses the connection with the management cosole, Disarmer continues to sanitize incoming files according to the definitions in the cached policy. Sanitization continues in this way, either until connection with the management Platform is restored, or until the time defined in NamedPolicyCacheInMin has lapsed. If the time lapses and no Management server is found, incoming files are all blocked.	The default is 1440 minutes (24 hours).
SdsApiToken	Defines the authentication token used by the Disarmer engine in every call to the Disarmer API. If you are using Votiro Disarmer for Email orVotiro Disarmer for File Transfer, you must set this token in the connector configuration file. If you are using the Votiro Disarmer API directly, you must set this token in the request header.	Token (such as GUID)

4.5.5 Sanitization API Settings

Use the apiservice.xml file to define attributes for the Votiro.Sanitization.API service.

The configuration file is located in:

`[installation_path]\Votiro\SDS Web Service\config.`

The attributes are described in Table 11 Sanitization API Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 11 Sanitization API Configuration File Attributes

Attribute	Comments	Value
SystemSettings		
MaxTempFileAgeInMin	Time after which the file is deleted from the TempFolder. See TempFolder on page 43.	The default value is 120 minutes. Do not change this setting unless instructed otherwise by Votiro.
QueueAdapterConfig		
MaxSecondsItemNotUsed	Maximum time within which API can receive a status request from a client before deleting the request.	The default value is 60 seconds. **Note** The maximum value permitted is 2147483.
QueuePollingTimeoutInSec	Time to spend in attempting to successfully receive a sanitization request from the queue.	The default value is 6 seconds. Do not change this setting unless instructed otherwise by Votiro staff.
MaxQueueCount	Specifies the maximum number of files that can be in the queue simultaneously for sanitization. After the maximum is reached, new requirements are not inserted into the internal queue. **Note** The value that you set affects performance and memory.	A positive integer. The default (and maximum value) is 1000.

4.5.6 Sanitization Node Monitor Controller (SNMC) Settings

Use the monitorservice.xml file to define attributes for the Sanitization Node Monitor Controller (SNMC).

The SNMC configuration file is located in [*installation_path*]\Votiro\SDS Web Service\config

The attributes are described in Table 12 SNMC Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

> **Note**
>
> Every sanitization node (SN) has a memory consumption limit, which is 75% of the machine's physical RAM. When the SN reaches its limit, the file in process will be blocked, as a protective measure. The total consumed memory across all SNs cannot exceed 100% of the machine's physical RAM. When required, machines can consume more than 100% of their physical memory by using virtual memory.

Table 12 SNMC Configuration File Attributes

Attribute	Description	Value
MonitorConfiguration		
FileName	The Sanitization Node Monitor Controller executable file. Do not change unless instructed by Votiro Support.	The default value is SdsSanitizationNode.exe.
PortBase	Defines the starting value for the serial range of port numbers to assign to the nodes. The range is then (PortBase+*number_of_nodes*-1). For example, if PortBase is set to 7871 and there are four sanitization nodes, then SNMC assigns the port numbers 7871, 7872, 7873, and 7874.	The default value is 7871. Ensure that the port range you assign is not in use in any process that is running on the computer where Disarmer is installed.
SanitizationTimeoutInSec	Defines the maximum amount of time a node can spend processing a single item.	The minimum value is 30. The default value is 1800.
KeepAliveSampleIntervalInMS	Defines the interval between keep-alive checks between SNMC and sanitization nodes.	The default value is 1000.
MemorySampleIntervalInMS	Defines how often SNMC queries the nodes' status. **Note** This setting might affect performance.	The default value is 500.

Attribute	Description	Value
DelayOnStartInSec	Defines after how many seconds SNMC queries the node status for the first time after initializing it. **Note** This setting might affect performance.	The default value is 30.
StatusRequestTimeoutInSec	Maximum number of seconds within which SNMC considers a note to still be responsive. The default value is 30. **Note** This setting might affect performance.	

4.5.7 Sanitization Node Settings

Use the sanitizationnode.xml file to define attributes for the Sanitization Node.

The Sanitization Node configuration file is located in [*installation_path*]\Votiro\SDS Web Service\config

The attributes are described in Table 13 Sanitization Node Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 13 Sanitization Node Configuration File Attributes

Attribute	Description	Value
QueueRunnerConfig		
QueuePollingTimeoutInSec	Time to spend in attempting to successfully receive a sanitization request from the queue. Do not change this setting unless instructed to by Votiro Support.	The default value is 6 seconds.

Attribute	Description	Value
EnableInProcessCleaning	Turns on and off a mechanism that cleans requests in the InProcess queue. ■ When true: The cleaner is on. A request that is still in the queue 24 hours after it enters will be removed. ■ When false: The cleaner is off.	The default value is true.

4.5.8 Scanner (Antivirus) Settings

Use the scanner.xml to define settings related to the Votiro Scanner service. The service controls the use of antivirus engines.

The scanner.xml file is located in:

`[installation_path]\Votiro\Votiro.Malware.Scanner\Config`

In the antivirus settings, you must specify a timeout value for the first antivirus update process. The initial antivirus update might take some time due to the size of the definition files that must be updated. During the time that this process is running, sanitization of files is blocked, meaning that performance is affected. Specify a timeout value that provides a balance between the need to have the latest virus definitions and the effect the process has on performance.

In addition, you must specify the update interval value and other attributes for each antivirus engine.

The attributes are described in Table 14 Scanner (Antivirus) Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 14 Scanner (Antivirus) Configuration File Attributes

Attribute	Description	Value
AntiVirusSettings		

Attribute	Description	Value
FirstUpdateTimeOutInSec	Specifies the length of time after which the first antivirus update process is timed out. Sanitization is suspended for the duration of the antivirus update. Performance is affected during this period. The minimum recommended timeout is 1200 seconds for low bandwidth internet links.	A positive integer representing the number of seconds after which timeout occurs and the update is stopped.
[*AntivirusApplicationName*] Settings		
IsActivated	Specifies the option to enable or disable the antivirus engine.	Either true or false. The default is true.
UpdateIntervalInMin	Specifies the frequency of checking for updates to the antivirus definitions.	A positive integer representing the number of minutes after which a check is made for new antivirus definition updates. The default is 15.
UpdateTimeOutInSec	Specifies the length of time after which the antivirus definition update process is timed out. This attribute does not apply to the first update.	A positive integer representing the number of seconds after which timeout occurs and the update is stopped. The default is 60.

4.5.9 SIEM Report Settings

Use the report.xml to define settings related to SIEM reports. The configuration file is located in two paths, corresponding to the two sources of reports that can be sent to a SIEM:

- The report.xml file for the Votiro Scanner Service is located in [*installation_path*]\Votiro.Malware.Scanner\Config.
- The report.xml file for all other Disarmer processes is located in [*installation_path*]\config

The attributes are described in Table 15 SIEM Report Configuration File Attributes. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 15 SIEM Report Configuration File Attributes

Attribute	Description	Value
SiemSettings		
IsActivated	Specifies the option to enable or disable the SIEM logging engine.	Either true or false. The default is false. Caution! The value that you set affects performance as each message is delivered over the network.
Format	Specifies the messages formatting of all messages delivered by the SIEM logging engine.	The default is CEF. It is the only valid value.
Address	Specifies the address or hostname of the SIEM system collector service.	A hostname where the address represents a fully qualified hostname or an IPv4 address. The default is empty. When the address is empty, the server uses its own IP as an address.
Port	Specifies the UDP port of the SIEM system collector service.	A positive integer between 1 and 65535. The default is 514.

4.5.10 Logs Settings

Use the logs.xml file to define the severity level of data that is logged, the number of files to back up, the maximum file size, and whether the logged information should be saved as a file or sent to Windows Event Viewer.

These settings are relevant to the following processes:

- Votiro.Sanitization.API
- Votiro.SNMC
- Sanitization Nodes
- Votiro.Sandbox

The logs configuration file is located in [*installation_path*]\Votiro\SDS Web Service\Config. In the case of the Votiro.Sandbox service, the logs file is in [*installation_path*]\Votiro\Sandbox\Config.

In addition to the logs that are configured in logs.xml, Disarmer logs can be sent to a SIEM in CEF format. For more information, see Sending Logs to SIEM in CEF Format on page 105.

The attributes that are described in Table 16 Log Configuration File Attributes and Table 17 Log Configuration Event Viewer Attributes appear in the logs.xml file. The tables provide a description of the attribute, considerations to make when specifying a value, and the permissible values.

The logs.xml attributes are divided into two tables, according to whether they relate to a log file or content that is being sent to the Windows Event Viewer.

> **Note**
>
> To apply changes to settings in the logs.xml file, you must save the file and restart the Votiro.Sanitization.API and Votiro.SNMC Windows services. This is true for all parameters except for LogLevel. In the case of LogLevel, immediately upon saving the file, the new log level is applied.

Table 16 Log Configuration File Attributes

Attribute	Description	Value
AppenderConfig		
LogLevel	Specifies the severity level of data that is logged. You can have more than one LogLevel attribute in the file. For example, you might choose to log Warning, Error, and Fatal events.	Values Any one of the following: Verbose, Debug, Info, Notice, Warning, Error, Fatal. Default is Debug.
NumberOfBackups	Specifies the number of files that can be backed up before file rotation occurs. When files are rotated, the first file that was created (the oldest file) is overwritten first.	A positive integer. Default is 10.
MaxFileSize	Specifies how large the log file can be before a new file is created.	A file size greater than zero, including the measurement being used, for example 40 MB (the default).

Attribute	Description	Value
FileName	Specifies the name of the file. Use ASCII characters when specifying a file name. Values The file name, in the format [*logname*].log, for example, sds.log. The default is *%Service%_%SdsVersion%_%ComputerName%*.log **Note** Do not change this setting unless instructed to by Votiro Support.	The default file name for sandbox logs is: VotiroSandbox_ *%ComputerName%* .log
FileFolder	Specifies the name and location of the folder where the log files are stored. If the value is empty, the folder is defined by the system as *%HomeDirectory%*\SDS Web Service\Logs. If you specify a value, it must be the full path of the folder. The default is Logs*%Service%.* **Note** Do not change this setting unless instructed to by Votiro Support.	The name of the folder, in the format [*drive*]:\[*path*]\[*folder*], for example, C:\Votiro\Logs\.
xsi:type	XML schema attribute. **Note** Do not change this setting unless instructed to by Votiro Support.	Default is File.

Table 17 Log Configuration Event Viewer Attributes

Attribute	Description	Value
AppenderConfig		
LogLevel	Specifies the severity level of data that is logged. You can have more than one LogLevel attribute in the file. For example, you might choose to log Warning, Error, and Fatal events.	Any one of the following: Verbose, Debug, Info, Notice, Warning, Error, Fatal. Default is Notice.

Attribute	Description	Value
ApplicationName	Specifies the name of the application that appears under Applications and Services in the Event Viewer.	The name of the application, for example SDS. You must use ASCII characters when specifying the application name. Default is SDS.
xsi:type	XML schema attribute. Default is EventViewer. **Note** Do not change this setting unless instructed to by Votiro Support.	

4.5.11 Active Directory

It is recommended to use the Management Platform to authenticate users. The Management Platform uses Active Directory for authentication.

IT personnel must define a group called Votiro_Users in Active Directory and add approved users with full permissions to the group.

To enable Active Directory verification in Management, provide the location of the Active Directory server and test the connection.

1. Launch Management.
2. In the dashboard, click **System Setup** in the navigation pane.
3. Click **Active directory**.
4. Type in the Active Directory location in the appropriate field.
5. Click **Test connection**.

   If the username and password are successfully authenticated to the Active Directory server, a check symbol appears next to the **Test connection** button and the **Save** button is enabled.
6. Click **Save** to save the settings, or **Reset** to clear them.

4.5.12 Sandbox Settings

Use sandbox settings to enable Votiro Disarmer to access your organization's sandbox. When access is enabled, you can configure Disarmer to direct unknown file types and binary files to the sandbox for additional handling.

The current implementation of the sandbox integration supports FortiSandbox by Fortinet, only.

The sandbox.xml file is located in:

[*installation_path*]\Votiro\Sandbox\Config.

The attributes described in Table 18 Sandbox Settings Configuration File Attributes appear in the sandbox.xml file. The table provides a description of the attribute, considerations to make when specifying a value, and the permissible values.

Table 18 Sandbox Settings Configuration File Attributes

Attribute	Description	Value
FortiSandboxSettings		
IsActivated	Enables access to FortiSandbox.	true to activate; false to deactivate
SandboxAddress	Specifies the location of the FortiSandbox server	Specify the location in the format: https://[*hostname*]:[*portnumber*] where hostname represents a fully qualified hostname. By default, SandboxAddress is empty.
UserName	FortiSandbox server username.	By default, UserName is empty.
Password	FortiSandbox server password.	By default, Password is empty.

Sandbox Port Value

Use the the Sandbox.WindowsService.exe.config file to set the value for SandboxServicePort, the port used for the sandbox.

The Sandbox.WindowsService.exe.config file is located in [*installation_path*]\Votiro\Sandbox. Add key under <appSettings> for <SandboxServicePort>. Ensure the value specified is set to the same value specified for the SandboxServiceAddress in Table 9 Machine Settings Configuration File Attributes.

Example

```
<appSettings>

. . .

      <add key="SandboxServicePort" value="4318" />

</appSettings>
```

> **Note**
> The values for <SandboxServicePort> and <SandboxServiceAddress> in the machine.xml configuration file, must be identical.

5 Using the Management Dashboard

The Management Dashboard enables you to perform the following procedures:

- Analyzing Sanitization Activity
- Exploring Incidents
- Configuring System Settings
- Managing Sanitization Policies
- Generating Reports

To log in to the Management Dashboard:

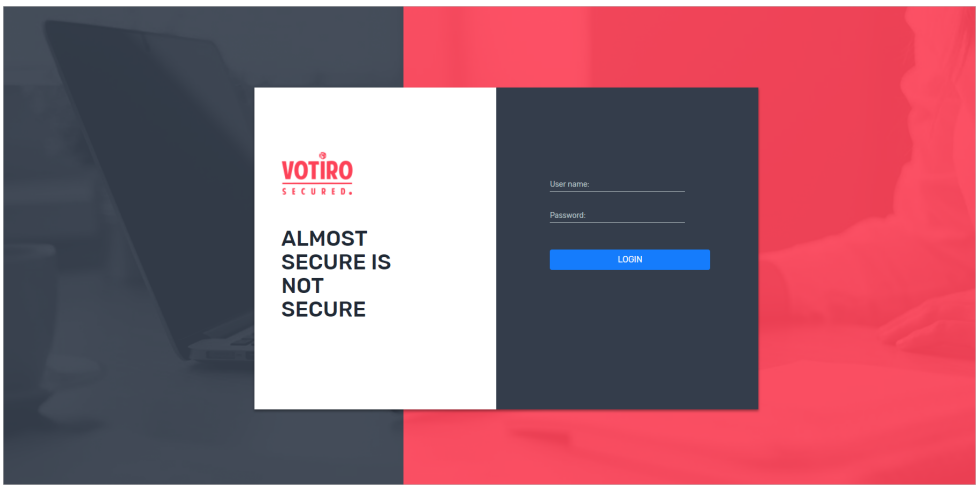
If you have configured the Management Platform to use Active Directory, only users that appear in the Active Directory group can log on.

1. On the server that is hosting the Management Platform, open a browser and navigate to:

   https://[*hostname*]:[*portnumber*]

   where *hostname* is the name of the server that is hosting the Management Platform. For more information, see Publishing and Storage Settings on page 40.

   The login screen is displayed:



2. Type in the username and password and click **LOGIN**.

> **Note**
> The Management Dashboard locks down for 10 minutes after three failed login attempt of a single username.

The Management Dashboard is displayed.

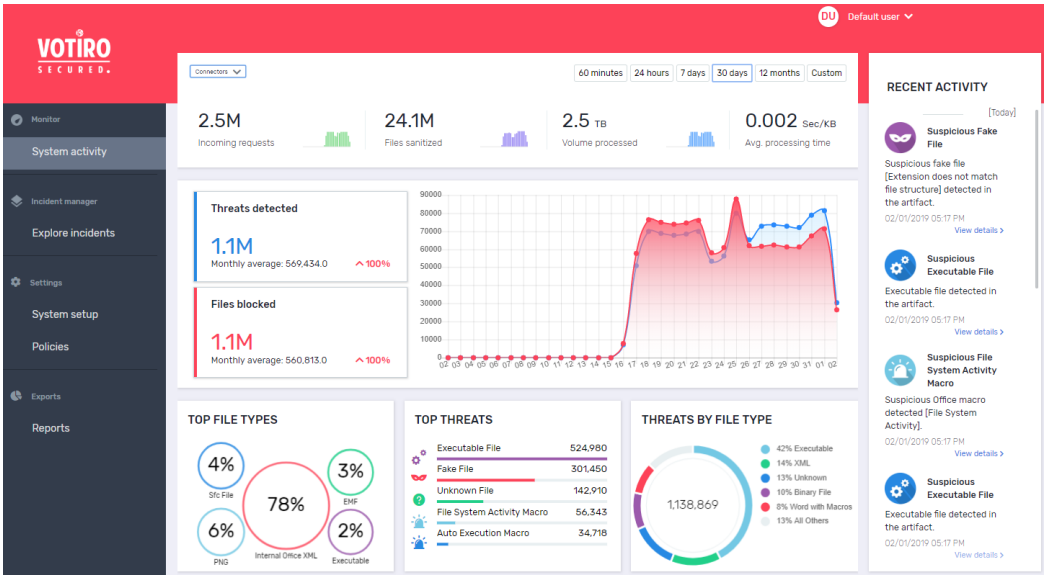
5.1 Analyzing Sanitization Activity

The System Activity page enables monitoring and analyzing of sanitization activity and provides a summary view of threats that were found in files that passed through the system.

A file is blocked or allowed according to the policy. A threat is detected regardless of the policy, whether the file was blocked or not.

There can be more than one recent activity message for a single file if it contains more than one threat. For example, the file can be both fake and contain a suspicious macro.

From the navigation pane on the left, click **System Activity**.



- **Central pane**: Displays statistics about the files that have gone through the system.
- **Right pane**: (Recent Activity) Displays a summary of the last ten files that were blocked.

5.1.1 Period Summary

The top area of the System Activity page is a summary of the selected period.

The following statistics are displayed:

Element	Meaning	Notes
1	Total number of requests incoming to Disarmer.	A single, flat file, or a nested archive are both single requests.
2	Total number of files that were sanitized by Disarmer.	The number includes root files and nodes.
3	Total volume that was processed by Disarmer.	
4	The selected time period.	See Periods on the next page.
5	Average time, in kilobytes per second for processing each item in the volume displayed.	
6	Total number of threats detected, with the average.	The average is calculated according to the period that is currently selected: an hourly average in the case of a 60-minute period, a daily average in the case of a 24-hour period, and so on.
7	Total number of files blocked, with the average.	Clicking on **Threats Detected** and **Files Blocked** displays the threats and blocked files in the Explore Incidents view. For more information, see Exploring Incidents on page 66.
8	Total number of zero-day attacks that were detected.	Clicking on **Zero-day attacks prevented** displays the affected files in the Explore Incidents view. For more information, see Exploring Incidents on page 66.
9	Graph showing threats detected and files blocked over the current time period.	
10	Summery for a specific time within the period.	

Periods

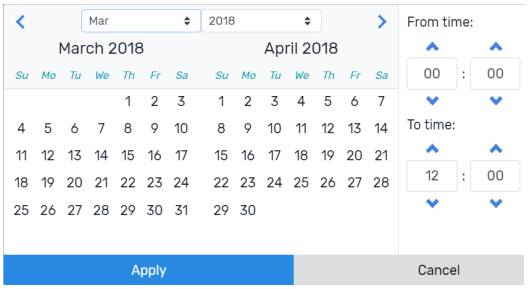
The statistics and graphs that are shown in the central pane of the System Activity page relate to the period that is currently selected. You can select a predefined period by clicking its button or define a custom period.

Votiro Disarmer provides the following predefined periods:

Period of Votiro Disarmer Activity	Meaning
60 minutes	The information is for the period starting 60 minutes earlier until the current time.
24 hours	The information is for the period starting from the beginning of the current hour, 24 hours earlier, until the end of the current hour.
7 days	The information is for the seven days that end at 23:59 of the current day.
30 days	The information is for the period starting from the current date, one month earlier, until the end of the current day.
365 days	The information is for the period starting from the beginning of the current month, one year earlier, until the end of the current month.

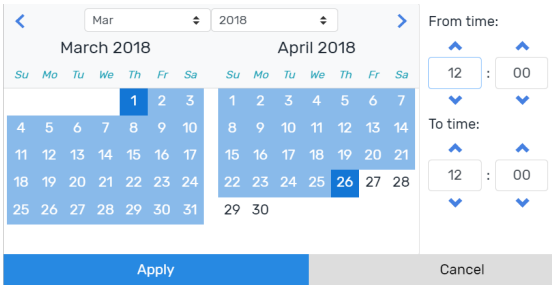
Defining a Custom Period

1. Click **Custom** to display the period selector.



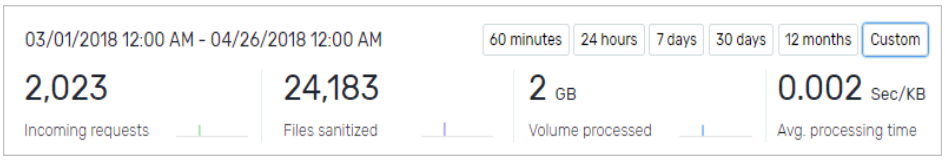
2. Navigate to the desired start month by clicking the right and left arrows or by selecting a month and year from the lists.
3. Select a start date.
4. Navigate to the desired end month.
5. Select a end date.
6. Select a time period.

The selected period is highlighted.



7. Click **Apply**

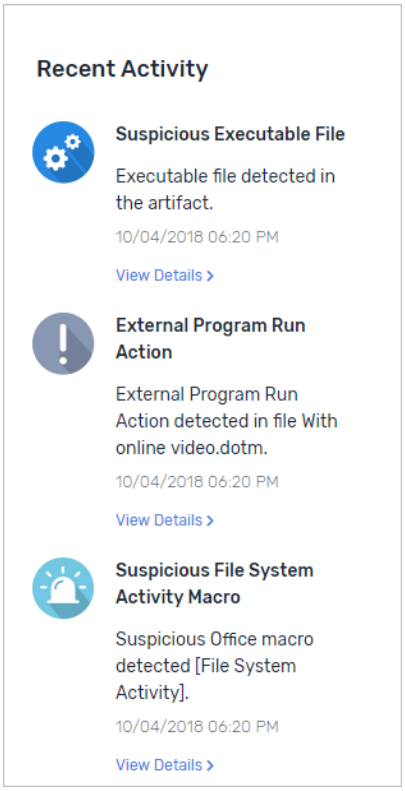
The custom period is displayed in the top left corner of the window:



Statistics and graphs update to show information for the custom period.

5.1.2 Viewing Recent Activity

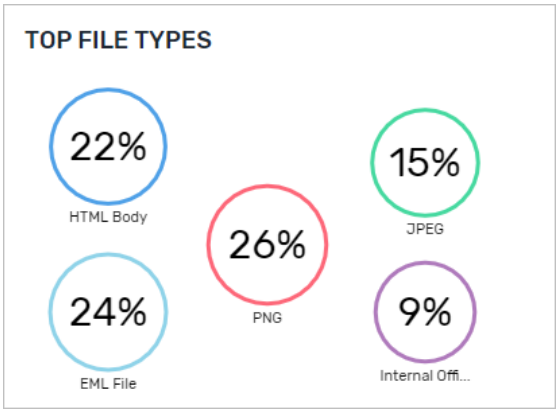
The Recent Activity pane displays the ten most recent file events.



Click **View Details** to view detailed information about the file, as described in Viewing Detailed File Information on page 65.

5.1.3 Viewing Top File Types

The Management Dashboard provides a graphic representation of the top five file types that have been sanitized during the selected period. The representation is according to percentages.

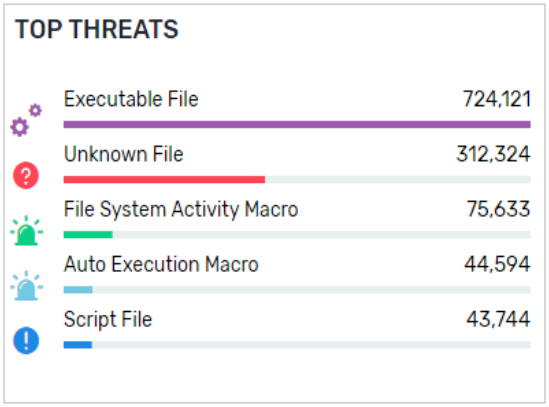


Click an area to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 66.

5.1.4 Viewing Top Threats

The Management Dashboard provides a bar chart representing the top five file threats that were detected during the selected period. The representation is according to the number of threats that were found.

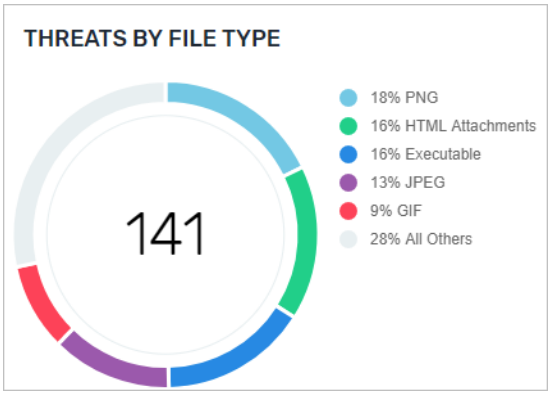


Click an item to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 66.

5.1.5 Viewing Threats by File Type

The Management Dashboard provides a pie chart representing the top five threats by file type that were detected during the selected period. The representation is according to the relative percentages of file types.



Click an area to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 66.

5.1.6 Zero-Day Detection

Votiro Disarmer protects your organization from zero-day attacks.

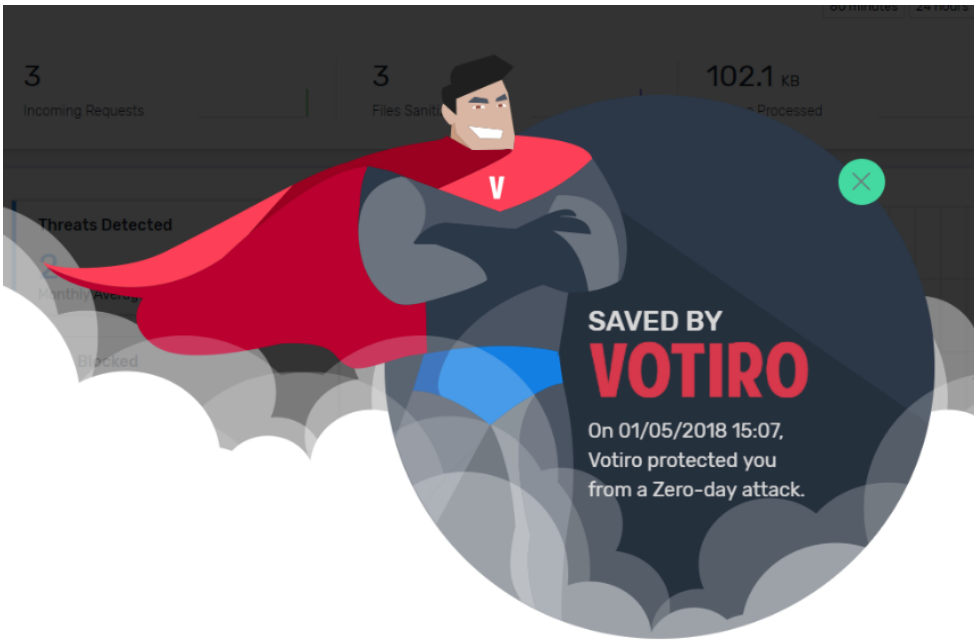
Votiro's Advanced CDR technology breaks down files into basic components, extracting from them all malicious content, and reconstructing them as a clean, safe-to-use files – without specifically identifying which files contain malicious code and which do not.

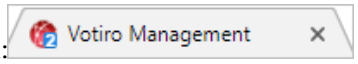
Disarmer periodically rescans the original files for viruses. New virus signatures cause the Antivirus to identify the original files that are infected with then-unidentified viruses.

Zero-day Detection Notifications

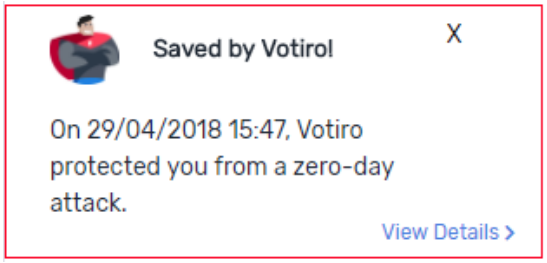
When Disarmer identifies a zero-day attack, it notifies you in several ways:

- It pops up the following notification in the Management Dashboard.



- A notification is added to the browser tab in which the dashboard is displayed: 

- In addition, a Saved by Votiro! item is added to the Recent Activity page:



  Click **View Details** to see detailed information about the file, as described in Viewing Detailed File Information on the next page.

- You can also configure the Management Platform to send an email notification to Votiro and/or staff in your organization each time a zero-day attack is detected. The email contains a link to the detailed information page of the malicious file.

For more information, see Zero-day detection Votiro notification on page 73 and Zero-day detection email notification on page 73.

5.1.7 Filtering Lists of Files in Storage

You can view a full list of filtered files that match an area of the System Activity page:

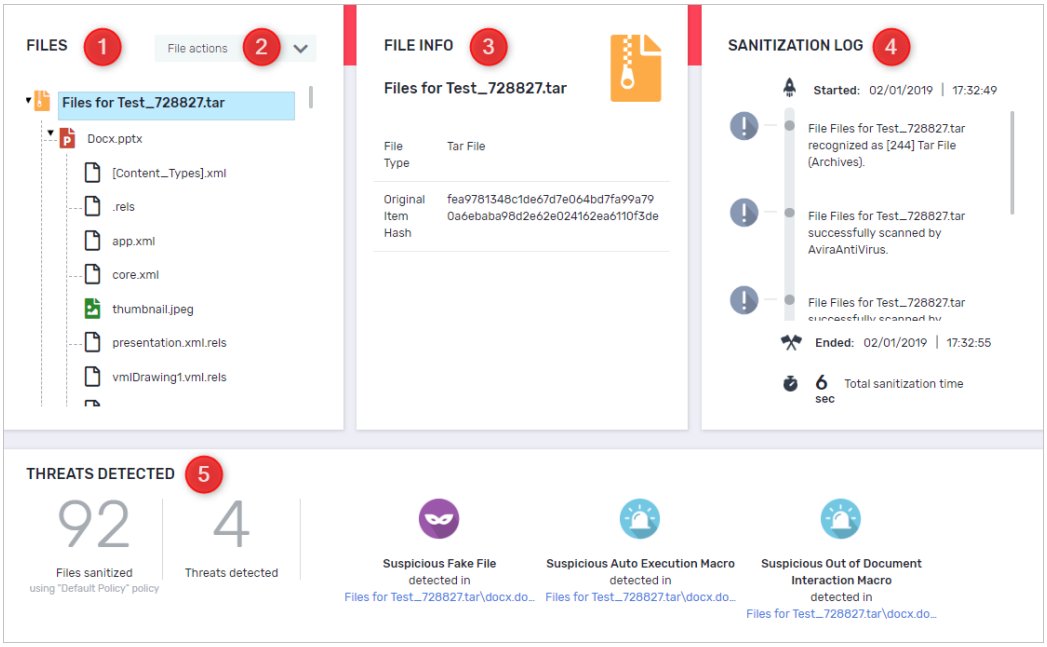
In the System Activity view, click	To see detailed file information in the Explore Incidents page about
Threats Detected	All threats that were detected.
Files Blocked	All files that were blocked.
A type in the **Top File Types**	All the files of the type selected.
A type in the **Top Threats**	All the files of the type selected.
A type in the **Threats by File Type**	All the files of the type selected.

In addition, clicking **View details** for a file in the **Recent Activity** panel displays details about the specific file in the Detailed File Information window, see Viewing Recent Activity on page 61.

For more information about the Explore Incidents page, see Exploring Incidents on the next page.

5.1.8 Viewing Detailed File Information

Detailed file information is displayed when you click **View Details** in the Recent Activity pane of the System Activity page, or **Details** for a file in the Explore Incidents page.



Element	Description
1	**Files**: Shows details of the file that you clicked in a previous window, in bold. The file is shown within the tree of its parents and children. The root is at the top. Scroll up or down in the pane; click the arrows to the left of the filenames to collapse and expand the nodes, as needed. Blocked files are shown in red.

Element	Description
2	The **File actions** list lets you perform the following actions for the file: ■ Explore Incidents. See Exploring Incidents below. ■ Download the original file. See Performing Actions on Files on page 68. ■ Download the sanitized file. See Performing Actions on Files on page 68. ■ Release the original file if it was blocked. See Releasing the Original Version of a Blocked Email on page 69.
3	**File Info**: Provides details about the file that is currently selected in the left pane. For all file types, the following is provided: ■ File icon ■ File name, or (in the case of an email) the subject ■ File type ■ Hash Additionally, for email files (EML and TNEF formats), the following is displayed: ■ From ■ To ■ CC ■ Received date
4	**Sanitization Log**: Provides sanitization log events that relate to the file that is currently selected in the left pane: ■ The date and time that sanitization began. ■ The date and time that sanitization ended. ■ A list of events during the sanitization of the selected file. ■ The total time taken to sanitize the selected file.
5	**Threats Detected**: Provides summary information about the entire tree – root and nodes – that is currently displayed in the left pane: ■ The total number of files that were sanitized. ■ The total number of threats detected. ■ A graphic, clickable representation of each threat is presented alongside.

5.2 Exploring Incidents

The Explore Incidents page provides a deeper look at files that were sanitized or blocked by the Disarmer Engine and that are currently stored on the Management server.

From the Explore Incidents page, you can download the original and sanitized files, as well as release files that have been blocked.

Accessing Explore Incidents

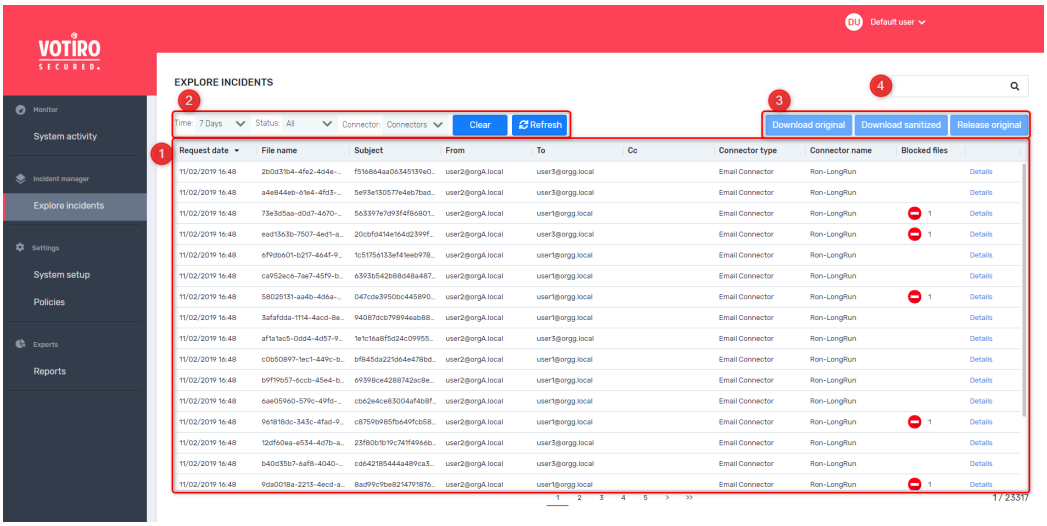
From the navigation pane on the left, click **Explore Incidents**.The *full* list of incidents that occurred in the last seven days is displayed.

Or

In the System activity view, click any of the following to see *the related details* in the Explore Incidents page:

- Threats detected
- Files blocked
- Top file types
- Top threats
- Threats by file types

For example, if you click **Files blocked** in the System activity page, the Explore Incidents page displays a filtered list of the files that were blocked.



Use this page to explore incidents (blocked and sanitized files) that occurred in the system. The page provides the following features:

Element	Description
1	Displays the file name, together with the date and time of the sanitization request. Double-click any file or click **Details** to see the file details in the Detailed View window.
2	Filters the list of files according to period and status. See Using Filters on the next page.
3	Perform actions on files. See Performing Actions on Files on the next page.

Element	Description
4	Perform a search on all the incidents in the blog. See Searching Sanitization Requests on page 70.

5.2.1 Understanding File Details

The sanitization requests (root files) that are currently stored on the Management server are listed in the main pane of the Explore Incidents page.

The following details are displayed for all requests:

- Request date
- File name: Root request file name.
- Connector type
- Connetor name
- Blocked files: Number of files in the file tree that were blocked.

For emails, additional details are shown:

- Subject
- From
- To
- CC

> **Note**
> The displayed requests might be filtered according to the manner in which you accessed the page. See Accessing Explore Incidents on the previous page.

To view file details, double-click any file or click **Details** in the sanitization request line. For more information, see Viewing Detailed File Information on page 65.

5.2.2 Using Filters

You can filter the file list in the following ways:

- Select from the **Status** list to view all files, blocked files, or sanitized files.
- Select an option from the **Time** list to filter according to a specific time period. Select **Custom** to define a range of dates. For instructions on how to define a custom period, see Defining a Custom Period on page 60.
- If you have more than one Disarmer Connector installed, you can filter the file list by connector type using the **Connector** list.

5.2.3 Performing Actions on Files

From the Explore Incidents page you can perform the following actions on the files in the blob:

- Download the file as it was before it was sanitized or blocked, by clicking **Download Original**.
- Download the sanitized version of the file by clicking **Download sanitized**.
- Release an original file that was blocked.

Releasing the Original Version of a Blocked Email

If an email has been blocked, you can release it from the blob and send it to one or more email recipients.

Usually, this procedure is performed by IT and only under unusual circumstances.

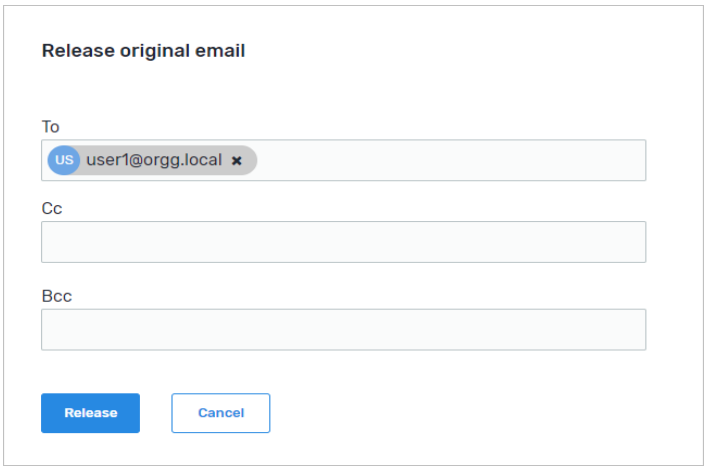
> **Note**
>
> To enable the release of blocked files, you must first configure the following system settings:
>
> - SMTP Server location
> - SMTP Server port
> - SMTP Server username
> - SMTP Server password
>
> For more information, see Configuring System Settings on page 71.

- If the released file is of type EML, the original sender's email address appears in the email that contains the attachment.
- If the released file is of another type, the email address of the user defined for the SMTP Server username setting appears as sender in the email that contains the attachment.

To release a blocked email:

1. Click an email file in the list of blocked files, then click **Release Original**.

   The following dialog is displayed:



   The dialog shows the same email addresses as were included in the original email, as well as their original designations: To, Cc, or Bcc.

2. Accept the email addresses that are displayed or delete one or more, as needed. You cannot add email addresses.

3. Click **Release** to send the email.

Releasing the Original Version of a Blocked File

If an file has been blocked, you can release it from the blob and send it to the OUT folder configured in Disarmer for File Transfer.

Usually, this procedure is performed by IT and only under unusual circumstances.

> **Note**
> To enable the release of blocked files, you must first configure the Management Platform in Disarmer for File Transfer.
> For more information, see Votiro Disarmer for File Transfer.

To release a blocked file, click a file in the list of blocked files, then click **Release Original**.

The original file is sent to the OUT folder.

5.2.4 Searching Sanitization Requests

You can search all the sanitization requests that are shown in the Explore Incidents page using the search bar. You can search by the following details:

- From (email only)
- To (email only)

- Subject (email only)
- Item ID: Specify an item ID in GUID (globally unique identifier) format.

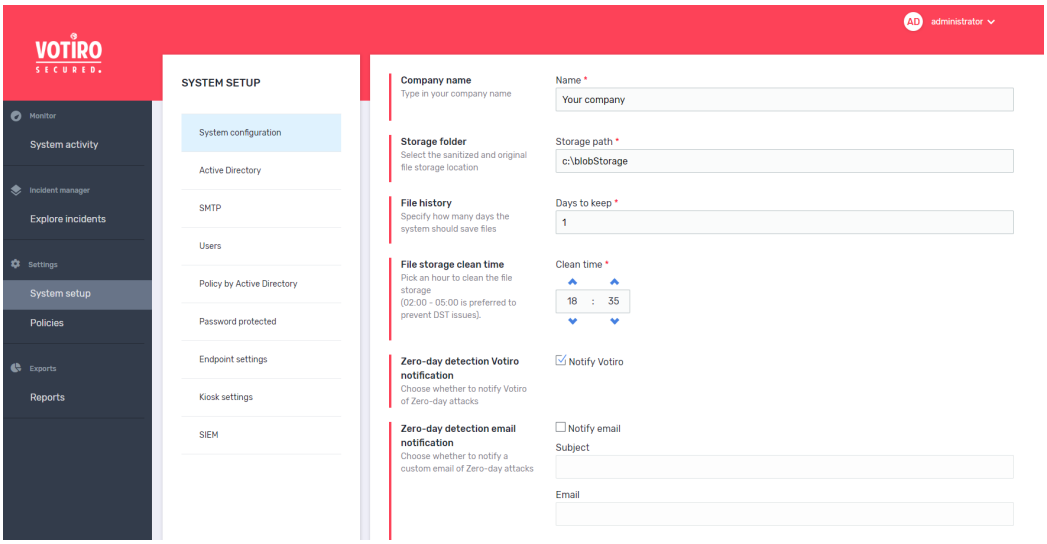
  This feature is useful for releasing a specific blocked files (see Releasing the Original Version of a Blocked Email on page 69). For example: An email that contains a file you are expecting has been blocked by Disarmer. As the recipient, you receive an email notification. The PDF file that is attached to the email message contains an item ID, such as the following:

  24c5e7cf-b8f8-4f64-a945-39c1a157a896

  To release the blocked file, copy and paste the item ID into the search bar and press Enter to display the file in the Explore Incident page. Select the file and click **Release original**.
- Sanitization request file name

5.3 Configuring System Settings

Use the System Setup page to configure settings in the Votiro Management Platform.



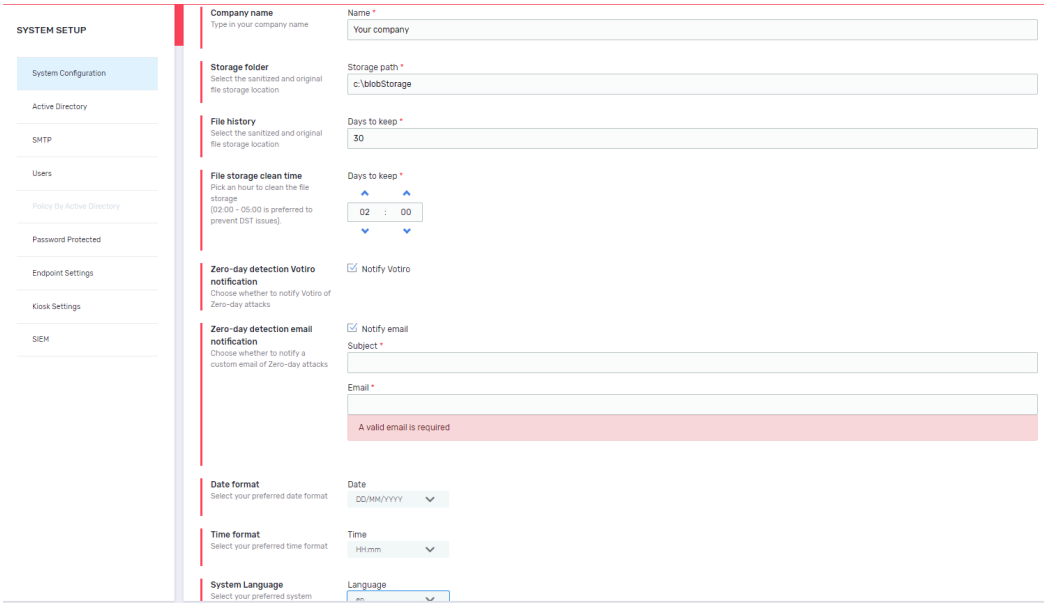
There are several active tabs in this view:

- System Configuration Tab
- Active Directory Tab
- SMTP Tab
- Users Tab
- Policy by Active Directory Tab
- Password Protected Tab
- Endpoint Settings Tab

- Kiosk Settings Tab
- SIEM Tab

> **Note**
> The Endpoint Setup and Kiosk Setup tabs only appear if you have these connectors installed.

5.3.1 System Configuration Tab

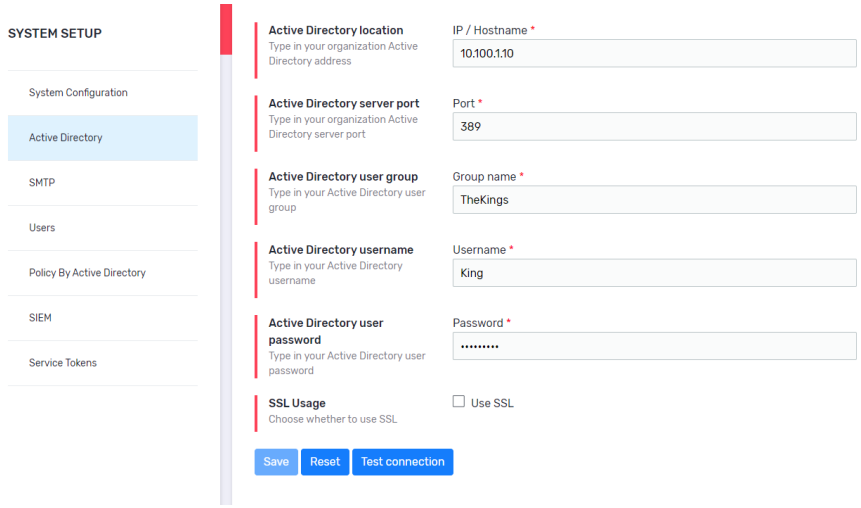


The System Configuration tab contains the following fields:

Field	Description
Company name	Specifies the name of your organization. The company name appears in activity reports. For more information, see Generating a Summary Report on page 1.
Storage folder	Defines the storage location of original and sanitized files. The default location is c:\blobStorage. **Note** It is highly recommended that the blob storage and operating system be in different locations.
File history	Specifies for how many days the system saves files. The default is 30.
File storage clean time	Specifies the time at which the Management Platform cleans the file storage. The recommended hours are between 02:00 and 05:00. The default is 02:00.

Field	Description
Zero-day detection Votiro notification	You can have the Management Platform notify Votiro each time a zero-day attack is detected. Select the **Notify Votiro** checkbox to activate notifications. The checkbox is selected by default. For more information, see Zero-day Detection Notifications on page 63.
Zero-day detection email notification	You can have the Management Platform notify someone in your organization each time a zero-day attack is detected. To activate notifications, select the **Notify email** checkbox and specify an email subject and recipient. For more information, see Zero-day Detection Notifications on page 63.
Date format	Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.
Time format	Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock format.
System Language	Select your preferred language. To add languages to the list you must translate Dashboard dictionary and upload the translation. Add a language to the Dashboard dictionary: 1 Navigate to the VotiroDisarmer server: ..\Votiro\Management\www\assets\i18n 2 Copy the English file **en.json** and save with a relevant. For example, **ja.json**. 3 Edit the copied file, changing display names as required. Save file. 4 Open file **locales.txt**. Add the name of your copied file. For example, **ja**. Do not use the extension. 5 In the Management Dashboard navigation pane, click **System Settings** > **System configuration**. The added language is now available for selection in the **System Language** dropdown.

5.3.2 Active Directory Tab

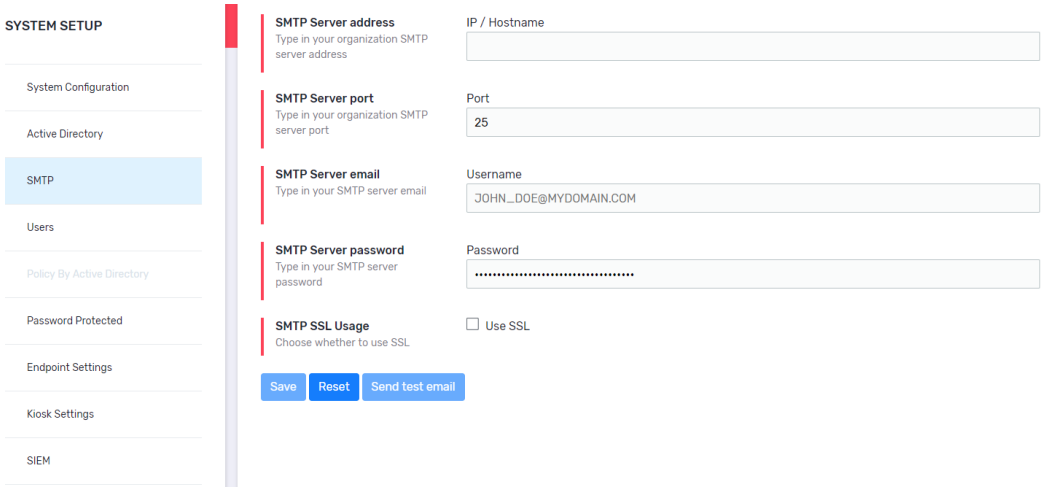


The Active directory tab contains the following fields:

Field	Description
Active Directory location	Specifies the Active Directory server that validates login.
Active Directory user group	Specifies the name of the Active Directory group. Only users that belong to the predefined Votiro_Users group in Active Directory can log onto Votiro Management Dashboard. For more information, see Active Directory on page 55.
Active Directory username	Specifies the login username for the Active Directory server.
Active Directory user password	Specifies the login password for the Active Directory server.

Before saving changes you must test the connection to Active Directory by clicking at the bottom of the screen.

5.3.3 SMTP Tab

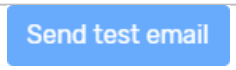


All SMTP settings are required to enable Management Platform features that rely on email. Configure SMTP settings to:

- Enable notifications about zero-day events. For more information, see Zero-day detection Votiro notification on page 73.
- Release original files from the blob. For more information, see Releasing the Original Version of a Blocked Email on page 69.

The SMTP tab contains the following fields for configuring the connection to an SMTP server:

Field	Description
SMTP Server address	Specifies the SMTP server that relays notifications from the Platform Management to users in your organization.
SMTP Server port	Specifies the SMTP server port.
SMTP Server email	Specifies the email address of the SMTP server user.
SMTP Server password	Specifies the password for the SMTP server user.
SMTP SSL usage	Select the **Use SSL** checkbox if you choose to use SSL over SMTP. The checkbox is unselected by default.

To test the SNTP settings, click 

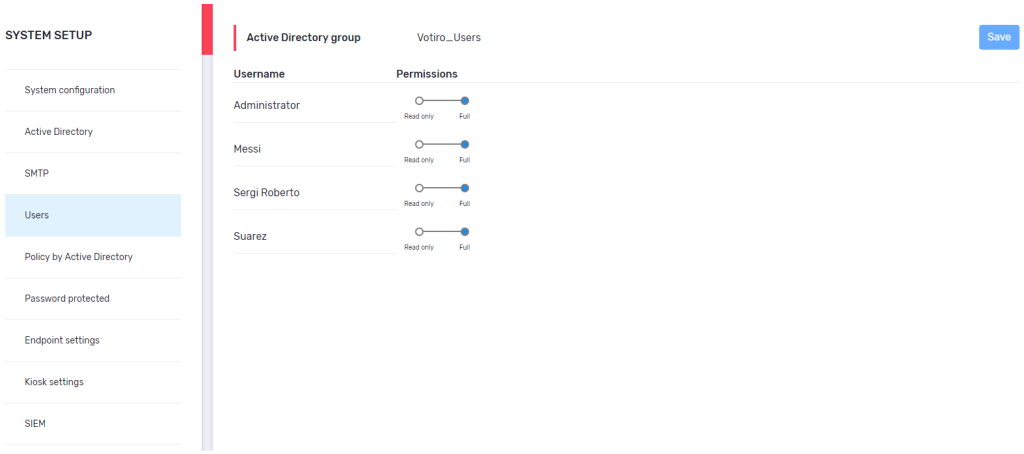
at the bottom of the screen.

- If the settings are valid, a verification code is displayed in the Management Dashboard.

  The same code appears in an email message that is sent to the address you specified.

- If the settings are invalid, an error is displayed below the button.

5.3.4 Users Tab



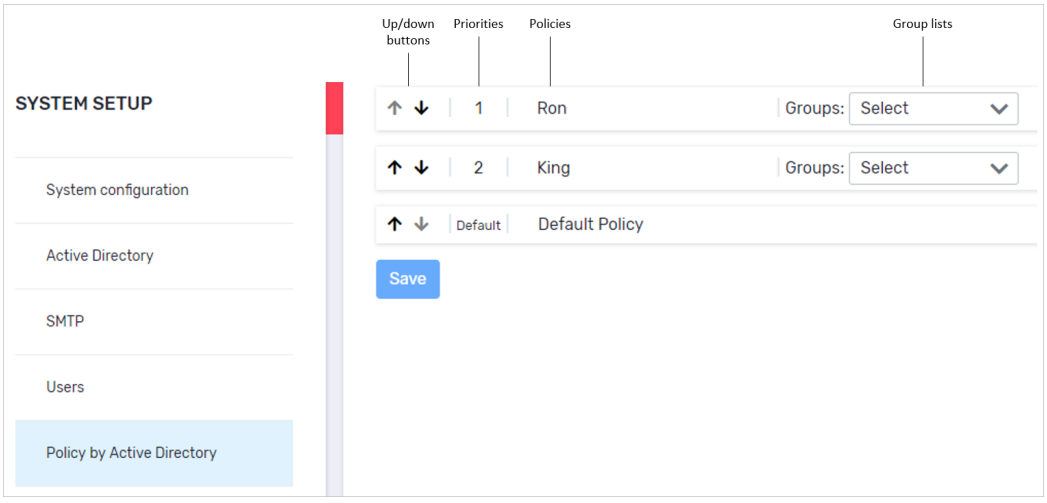
The Users tab enables you to define permissions for users of the Votiro Management Platform.

Users must be in the Votiro_Users Active Directory group.

- Read-only users will only be able to view the dashboard. They will not have access to personal data, or be able to change settings.
- Full-permission users will have access to the entire system, including personal files and emails, policy configuration, system settings and Users screen.

For each user, select **Read only** or **Full**.

5.3.5 Policy by Active Directory Tab



Organizations that use Active Directory often assign users to Active Directory groups. For example, IT, QA, RnD, Marketing, Product, Management, Finance, HR.

The Policy by Active Directory feature enables setting a sanitization policy to each Active Directory group and set priorities for those policies.

Once the order of priorities has been set, incoming emails or files that are earmarked for users are processed accordingly. For each incoming item, Disarmer looks for the first Active Directory group that matches the intended user and applies the policy that was assigned to it.

Examples

- A Security department in an organization wants to keep track of files entering the organization and analyze each event. The policy that would best suit their needs would allow the Security Active Directory group (and only them) to receive malware to their isolated environment.
- Finance department personnel often use macros to perform their daily tasks. An appropriate policy for the Finance Active Directory group would allow them to receive Excel files that contain macros. For the rest of the organization, the policy would remove the suspicious macros.

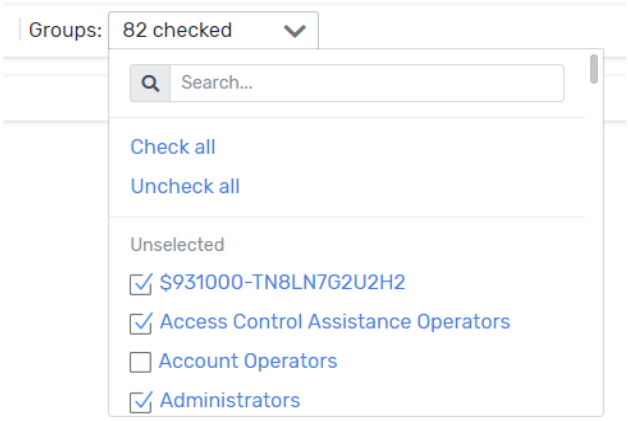
To assign groups to policies and prioritize the policies:

1. In the Management Dashboard navigation pane, click **System Settings**, then click **Policy by Active Directory**.

   A table of the policies that have been defined is displayed. There are three elements for each policy:

   - **Priority**: Displays the current priority of the policy. Use the up and down arrows to set the priority. The policy with first priority ("Ron" in the image above) is the most lenient; the policy with last priority (for "Default Policy") is the most restrictive.
   - Policy name
   - **Groups**: Contains a list of the groups that are defined on the Active Directory server. Select a groups from the list to assign the policy to them.

When you click the list, the following appears:



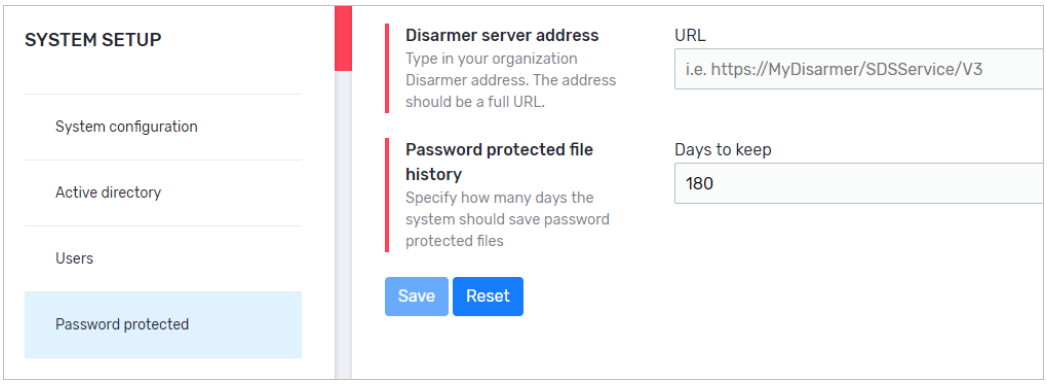
Check a group to select it. There are buttons to check all groups and uncheck all groups.

You can also search for a group by typing its name in the Search field.

2. Click **Save**.

5.3.6 Password Protected Tab

Use the Password Protect tab to configure settings for the management of password-protected files.



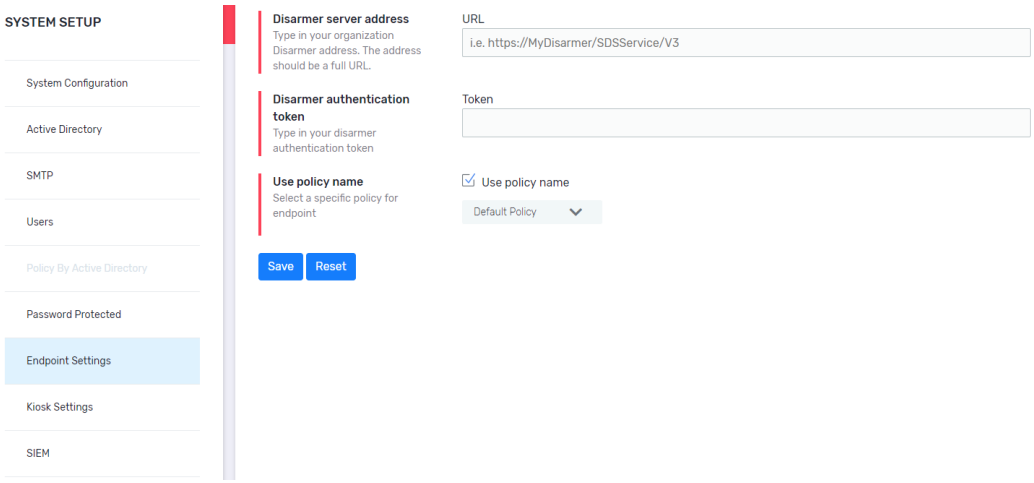
The Password Protect tab contains the following fields:

Field	Description
Disarmer server address	Specifies the address of the Disarmer server to use. The address must be in the format: https://MyDisarmer/SDSService/V3

Field	Description
Password protected file history	Specifies for how many days the system saves password-protected files. The default is 180. **Note** After the configured period, the original file is deleted and cannot be retrieved through the dashboard.

5.3.7 Endpoint Settings Tab

If you installed the Disarmer for Removable Devices app, use the Endpoint Settings tab to configure communication with the Disarmer server and select the sanitization policy to use.

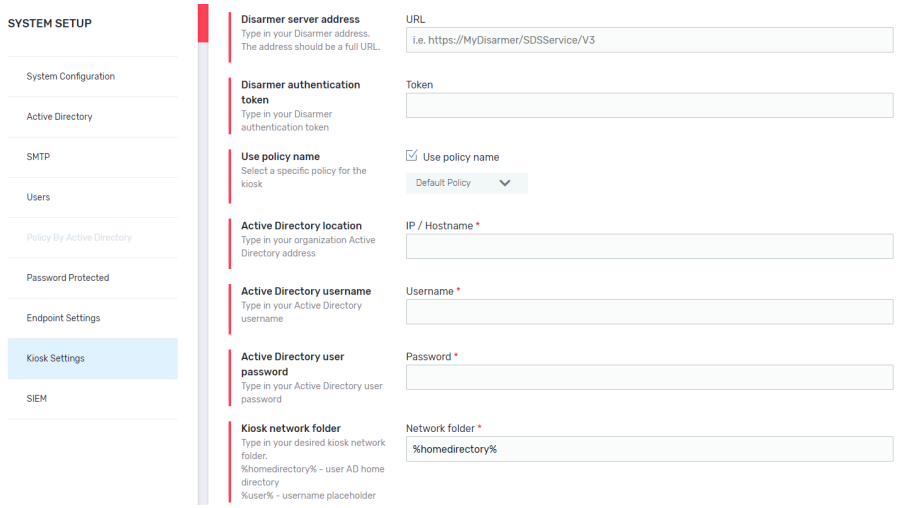


The Endpoint Settings tab contains the following fields:

Field	Description
Disarmer server address	Specifies the address of the Disarmer server to use. The address must be in the format: https://MyDisarmer/SDSService/V3 **Note** The Disarmer server address must be complete for the Test File feature to work.
Disarmer authentication token	If Disarmer is using HTTPS communication, specify a value for the Disarmer authentication token, otherwise leave blank.
Use policy name	To use a set policy, check the **Use policy name** checkbox, then select a policy from the list. If **Use policy name** in unchecked, a policy by active directory is used.

5.3.8 Kiosk Settings Tab

If you have a Votiro Kiosk installed, use the Kiosk Settings tab to configure relevant settings in the Management Platform.



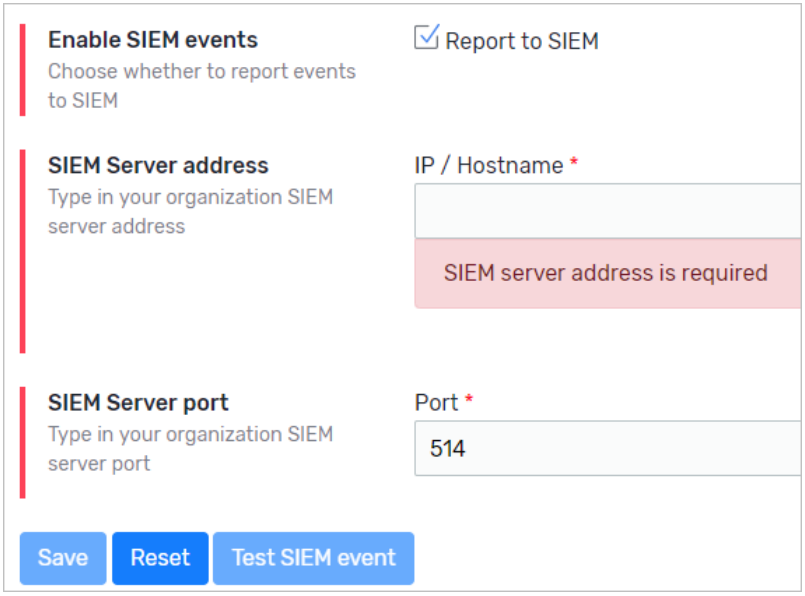
The Kiosk Settings tab contains the following fields:

Field	Description
Disarmer server address	Specifies the address of the Disarmer server to use. The address must be in the format: https://MyDisarmer/SDSService/V3
Disarmer authentication token	Defines the authentication token that will be recognized by Disarmer during the process of publishing to the Votiro Management server.
Use policy name	■ When the **Use policy name** checkbox and policy from the list are selected, all Kiosk users are bound by the selected policy. ■ If the checkbox is unselected, Kiosk users are bound to the policies that are assigned to Active Directory groups. For more information, see Policy by Active Directory Tab on page 76.
Active Directory location	Specifies the Active Directory server that validates login.
Active Directory username	Specifies the username of the Active Directory server administrator.
Active Directory user password	Specifies the password of the Active Directory server administrator.

Field	Description
Kiosk network folder	Specifies the network folder in which to write sanitized files. There are three configuration options: ■ (Default) Specify %homedirectory%. This setting assumes that in the Active Directory server, both the current user and a personal /<*user*> network folder have been defined. Sanitized files are written to that folder. ■ Specify a network shared folder path. If this setting is specified, all users using Kiosk have a network folder enabled and sanitized files are written to that folder. ■ Specify a network shared folder path and add \%user%. If this setting is specified, a /<*user*> folder is created under that network drive and sanitized files are written to it.

5.3.9 SIEM Tab

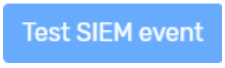
Use the SIEM tab to configure settings for the saving Management event logs in a SIEM.



The tab contains the following configuration fields:

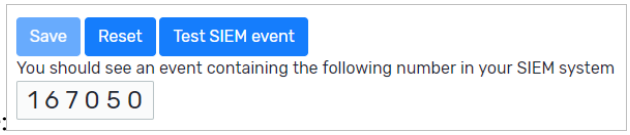
Field	Description
Enable SIEM events	To activate SIEM logging, select the **Report to SIEM** checkbox.
SIEM Server address	Address of the SIEM system collector service. Specify a hostname where the address represents a fully qualified hostname or an IPv4 address. The default is empty. When the address is empty, the server uses its own IP as an address.

Field	Description
SIEM Server port	Specifies the UDP port of the SIEM system collector service. Specify a positive integer between 1 and 65535. The default is 514. For more information about SIEM logging in Management, see Sending Logs to SIEM in CEF Format on page 105.

To test the connection settings , click 

at the bottom of the screen.

- If the settings are valid, a verification code is displayed in Management. For example:



  The same code should appear in your SIEM system.

- If the settings are invalid, an error is displayed below the button.

5.4 Managing Sanitization Policies

5.4.1 About Sanitization Policies

A sanitization policy defines the manner in which an organization handles a file matching a set of criteria that enters its network. The policy can determine how files are sanitized, including whether files are blocked or permitted.

For example, your organization's sanitization policy might comprise the following rules:

- Sanitize all image files and rasterize vector images.
- Block all fake files and customize the block message that the end user receives to be "Due to a recent spike in threats associated with fake files, the company has decided to block them."
- Sanitize all PDF files, except if they are larger than 25 MB. In such an event, the file is blocked.

Votiro Disarmer uses policy definitions that are defined in the Management Dashboard.

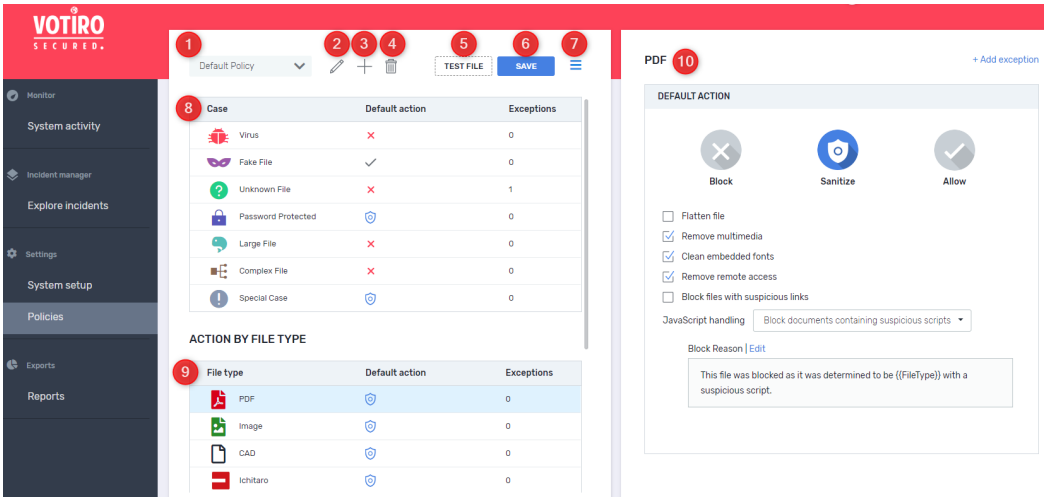
If you do not create a customized policy, the Disarmer engine uses a set default policy.

If you have custom, XML-based policy definitions, you can load these to the Management Dashboard as special cases. To learn how to include special cases, see Defining Policy Based on Special Cases on page 95.

5.4.2 Managing Sanitization Policies Dashboard

The Policies view in Votiro Management lets you create, edit, and manage the sanitization policies that operate in the Disarmer Engine.

From the navigation pane on the left, click **Policies**.



Element	Meaning
1	The name of the currently displayed policy. To display a policy, select from the list of defined policies.
2	Edit the policy name
3	Add a new policy
4	Delete current policy
5	Select file to test policy. **Note** Set the Disarmer server address in Endpoint Settings for this to work.
6	Save current policy
7	Import/Export policy file
8	Displays the details of the selected policy by case
9	Displays the details of the selected policy by file type
10	Displays details of the item that is selected on the left. For each case or action, you can define how it must be handled.

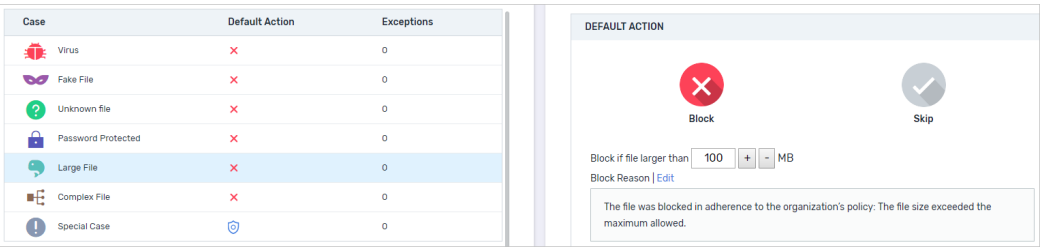
> **Note**
> Change made in policies are updated in the Disarmer Engine every few seconds. Once updated in the Disarmer Engine, it is available to Disarmer reference clients, such as Votiro Disarmer for Email or Votiro Disarmer for File Transfer.

5.4.3 File Blocking

When you configure a policy to block a file, no other policy rule is applied on the file. A block file containing information about the blocked file and the reason it was blocked replaces the original file You can accept the block file default text or edit it.

A block file is a document that replaces an original file that was blocked. The block file is attached to an email and can be customized for each company and for each set of criteria.

5.4.4 Defining Policy by Case



When defining a policy by case, you can perform the following actions:

- Block the file
- Skip the file
- Add one or more exceptions to the policy. For more information, see Defining Exceptions on page 96.

If you choose to block the case, you can:

- Set additional options if they are provided (as in the image above)
- Edit the default block reason text

After you save the settings for the case, the display updates to show the action symbol in the Default Action column and the number of exceptions in the Exceptions column.

The following table describes the sanitization options that are available for each case:

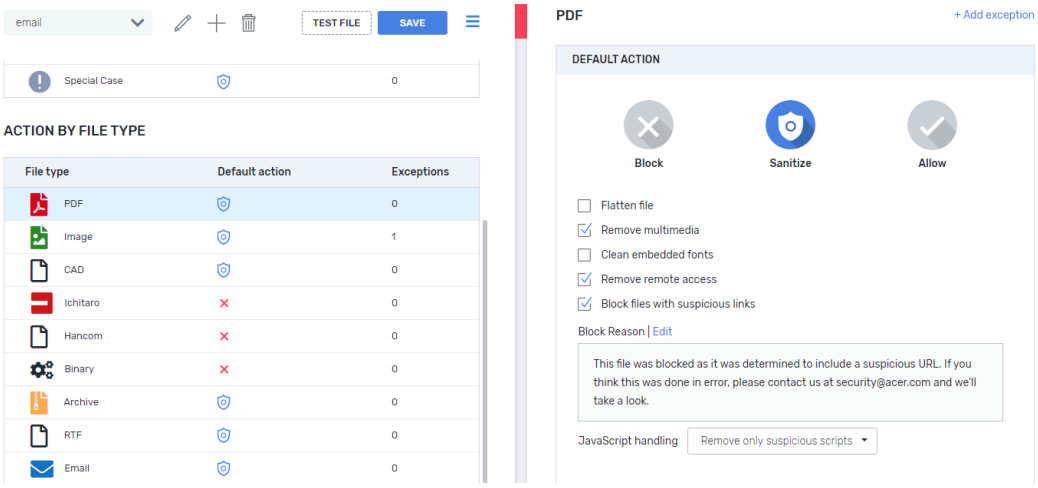
Table 19 Sanitization Options for Cases

Case	Description	Sanitization Options
Virus	Specifies which antivirus engines scan the files for malware.	■ Scan files using Avira antivirus ■ Scan files using Windows Defender antivirus (available only if Windows Defender antivirus is enabled in the servers hosting Disarmer and the Management Platform) **Note** If none of the options is checked, antivirus scanning is skipped.
Fake File	Specifies how to handle any file whose extension does not match the file type.	By default, the check for fake files is skipped, but the files themselves undergo full sanitization -- fake files thus pose no threat at all.
Unknown File	Specifies how to handle data files or unidentified file types.	You can block or skip these. If you select Skip, the unknown file is not sanitized and the original version will reach the destination folder. Select the **Send all unrecognized files to Fortinet sandbox** to send unknown files to Fortinet's sandbox. **Note** Processing by the sandbox might affect performance.

Case	Description	Sanitization Options
Password Protected	Specifies how to handle password-protected files.	You can block or sanitize these files. By default, the files are sanitized. When the files are blocked, Disarmer issues a block-file containing the reason it was blocked. The notification contains a link that opens a web page where the password can be entered. When the correct password is entered, the blocked file returns to the Disarmer server, and is sanitized. The sanitized file is then downloaded to the user's computer, or sent by email as an attachment. The password protection case in the Management Dashboard provides: ■ A checkbox that enables you to return the file by email. If the source of the file was an email attachment, the sanitized file will be returned to all recipients as an email attachment. ■ A user message that appears in the notification. Accept the default text or edit it. ■ A checkbox that enables you to block unsupported files (such as Visio files). **Note** This feature supports the following file types only: PDF, ZIP, 7zip, RAR, DOC, DOCX, DOT, DOTX, DOCM, DOTM, XLS, XLT, XLSX, XLTX, XLSM, PPT, PPS, POT, PPTX, PPSX, POTX and PPTM. It does not work on other file types that can be protected by a password, such as Visio files. ## Instructions for Email User The Disarmer administrator should communicate the following information and instructions to the users. An email message with password protected files attached can be sanitized and returned as an email attachment, or as a download. The user receives a message on screen that a password protected file has been received. The

Case	Description	Sanitization Options
		user inputs the password and clicks **Get File**. The password protected file is sanitized and attached to the email. This is distributed to all named recipients. If Disarmer has already sanitized and returned password protected files, additional users requesting files to be sanitized will be advised that sanitzation has already taken place. **Note** This feature supports the use of one password per email.
Large File	Specifies how to handle large files.	You can set the minimum size of files you want to block. When this option is checked, for every file that Disarmer blocks, it issues a block-file containing the reason it was blocked. Accept the default text or edit it.
Complex File	Specifies how to handle nested files.	You can set a layer number. Files that are found in that layer or deeper are blocked.
Special Case	Specifies a custom policy.	You can load a special case policy, created externally. For more information, see Defining Policy Based on Special Cases on page 95.

5.4.5 Defining Policy by File Type



When defining a policy by file type, you can perform the following actions:

- Block the file under all conditions. You can edit the default notification about the blocked file.
- Sanitize the file using default sanitization settings. You can modify the default behavior by setting options when they are provided (for example, as in the image above). You can also edit the default block reason text.
- Allow the file under all conditions.
- Add one or more exceptions to any of the previous three settings. For more information, see Defining Exceptions on page 96.

After you save the settings for the file type, the display updates to show the action symbol in the Default Action column and the number of exceptions in the Exceptions column.

The following table describes the sanitization options that are available for each file type:

Table 20 Sanitization Options for File Types

File Type	Description	Sanitization Options
PDF	Specifies how to sanitize PDF files. **Note** For managing the compression level when processing flat streams in PDF files see Compression Levels on page 95.	By default, these files are sanitized. ■ **Flatten file**: Flattens PDF documents, preserving reading and editing capabilities. Default is unchecked. **Note** If you have selected **Flatten File**, other options are unavailable. ■ **Remove multimedia**: Specifies whether multimedia such as embedded video, audio, 3D annotations, and rich media annotations must be removed. Default is checked. ■ **Clean embedded fonts**: Specifies whether embedded fonts must be sanitized. Default is checked. ■ **Remove Remote Access**: Specifies whether communications to an external server must be disabled. Default is checked. ■ **Block files with suspicious links**: Performs a check of all HTTP:// and HTTPS:// links. If a link is found to be suspicious, the file is blocked. When this option is selected, for every file Disarmer blocks, a block-file containing the reason it was blocked is issued. You can edit the default block reason. Default is unchecked. **Note** When **Blocked files with suspicious links** is selected ensure the machine.xml configuration file has CloudVotiroSettings enabled. ■ **JavaScript handling**: Determines how JavaScript, if found in the PDF file, is handled. ♦ Don't do anything. ♦ Remove only suspicious scripts. ♦ Remove all scripts (this is the default). ♦ Block documents containing suspicious scripts.

File Type	Description	Sanitization Options
Image	Specifies how to handle image files.	By default, these files are sanitized. ■ **Rasterize vector images**: Converts vector images to raster images. Default is unchecked. ■ **Add micro-changes**: Adds security noise to images during sanitization. Default is checked. **Note** Increasing the noise level might enlarge the sanitized files, particularly in the case of png files. Unselecting noise level (off) usually preserves an image file size. ■ **Remove metadata**: Removes EXIF metadata from JPEG and TIFF images. Default is unchecked. ■ **Max compression for lossless formats**: Compresses lossless image formats (PNG, BMP, and RAW) by 100%. Default is checked. ■ **Compression level**: The sanitized image is compressed to preserve a reasonable image file size. You select one of five compression levels (from 0% to 100%) that trade off file size with image quality – the larger the file, the higher the image quality. Default is 25%.
CAD	Specifies how to handle DWG, DWS, DWT, DXF, JWW, SFC, and P21 files that were created using CAD software. The files are re-generated, preserving layers and structure.	By default, these files are sanitized. ■ **Remove VBA macro**: Removes embedded VBA macros. Default value is checked.

File Type	Description	Sanitization Options
Ichitaro	Specifies how to handle Ichitaro documents and their embedded objects. The supported Ichitaro document versions are: ■ For JTD files: Ichitaro Pro 3/Pro 2/Pro/Government 8/Government 7/Government 6/2017-2004/13-8 ■ For JTDC files: Ichitaro Pro 3/Pro 2/Pro/Government 8/Government 7/Government 6/2017-2004/13-11. **Note** ■ Ichitaro sanitization requires that Votiro Disarmer be installed on Japanese locale Windows server. Applying Ichitaro sanitization policy action on non-Japanese locale system will result in unexpected behavior. ■ Ichitaro sanitization cannot be performed on the same server where JUST Office or Ichitaro is installed. Applying Ichitaro sanitization PolicyAction on the same Windows instance where JUST Office or Ichitaro is installed will result in unexpected behavior.	By default, these files are sanitized. ■ **Remove Macros**: Default is checked. ■ **Preserve original Ichitaro OLE objects**: Preserves OLE controls and OLE sheets. Default is checked.

File Type	Description	Sanitization Options
Hancom	Specifies how to handle Hancom Office files. **Note** Hancom .HWP 3.0 files are not supported.	By default, these files are sanitized. - **Remove Macros**: Default is checked. - **Remove scripts**: Default is checked.
Binary	Specifies how to handle binary files.	The Sanitze option is not relevant to managing binary files. You either block binary files or allow them. - **Allow**: A binary file will not be sanitized. Select **Send binary files to Fortinet sandbox** to send binary files to Fortinet's sandbox. If this option is not selected, the original version will reach the destination folder. **Note** Processing by the sandbox might affect performance.
Archive	Specifies how to handle archives.	By default, these files are sanitized. **Block zip bomb**: Detects and blocks zip files with abnormal compression ratio. These might pose a denial of service threat, consuming system resources such as CPU or disk. Any zip files with compression ratio higher than 99.8% will be considered a zip bomb and be blocked. Default is checked.
RTF	Specifies how to handle RTF files.	By default, these files are sanitized. There are no sanitization options.

File Type	Description	Sanitization Options
Email	Specifies how to handle email files. Sanitization is on EML files and their attachments. **Note** Each attached file is processed recursively by running all policy rules on it.	By default, these files are sanitized. ■ **Block files with suspicious links**: Performs a check of all links in the form HTTP:// and HTTPS:// in the body and attachments of an email. If any link is found to be suspicious, the email body or attachment is blocked. Default is unchecked. **Note** If you have checked **Blocked files with suspicious links**, ensure the machine.xml configuration file has CloudVotiroSettings enabled. ■ **Convert HTML body to text**: Converts EML files with HTML body into text body emails. For more information, see Converting HTML to Text Emails on page 104. Default is unchecked. ■ **Add footer**: Adds a footer. Default is checked. Accept the default footer for HTML-based emails and/or text-based emails or edit it.

File Type	Description	Sanitization Options
Microsoft Office	Specifies how to handle Microsoft Office files. Sanitization applies to Microsoft Office files and their embedded objects. **Note** Each attached file is processed recursively by running all policy rules on it.	By default, these files are sanitized. ■ **Block files with suspicious links**: Performs a check of all links in the form HTTP:// and HTTPS:// in Microsoft Word files. If any is found to be suspicious, the file is blocked. Default is unchecked. **Note** If you have checked **Blocked files with suspicious links**, ensure the machine.xml configuration file has CloudVotiroSettings enabled. This option is available for DOC/DOCX file types only. ■ **Macro handling**. In the list, choose one of the following: ♦ **Don't do anything** ♦ **Remove only suspicious macros**: Remove all macros only if any suspicious code is found. ♦ **Remove all macros**: Remove all macros from the document. This is the default option. ♦ **Block documents containing suspicious macros**: Block the entire document if suspicious code is found in the macro. **Note** Excel files with "4.0 macro" (also known as "sheet macro") are automatically blocked. It is common practice to use VBA macros. Excel files with VBA macros are checked for suspicious code (see options above). ■ **Remove metadata**: Removes metadata, such as Author, Company, LastSavedBy, and so on. Default is unchecked. ■ **Remove printer settings**: Removes the printerSettings1.bin (printer settings) embedded in a .xlsx file. Default is checked. ■ **Remove OLE**: Removes OLE controls including attachments. Default is unchecked. Changing this setting is not recommended and might affect the sanitized files.

File Type	Description	Sanitization Options
		■ **External program action handling:** Removes *either*: ♦ Objects that have potentially malicious links for example, OLE links and DDE, in all Office files (except Visio files). From the list, select one of the following: ● **None** ● **Remove or Block document**: Block the entire file if an OLE link is found in an Office file. The default is Remove. *OR* ♦ External actions in PowerPoint files. From the list, select one of the following: ● **None** ● **Remove**: Remove all external actions. This is the default. ● **Block document**: Block the entire file if an external action is found.
Text	Specifies how to handle text files.	By default, these files are sanitized. **Block CSV with threat formula**: Blocks CSV files that contain formula injections. Default is checked.
Other files	Specifies how to handle unsupported files.	By default, these files are blocked. There are no sanitization options.

Compression Levels

You can determine the level of compression required when processing flat streams, such as content streams and PNG images. You can set a value between 0 (minimum compression) and 9 (maximum compression), this will impact the size of the file output. The default value is 6.

> **Note**
> Compression Level is defined as a Special Case in the **Defining Policy by Case** section, see Defining Policy Based on Special Cases below.

5.4.6 Defining Policy Based on Special Cases

You can load a specific policy requirement as a special case, also known as a *custom policy*. A **special case** type policy is created outside of the Management Dashboard, and added in this section.

We recommend this feature is used for specific requirements only. For more information, contact Votiro Support.

5.4.7 Defining Exceptions

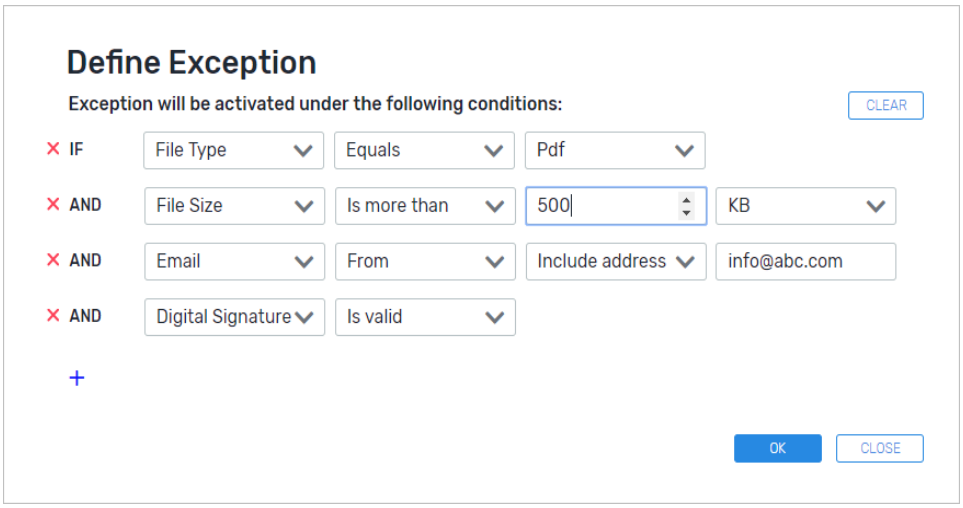
You can define one or more exceptions to any case policy or file type policy. Exceptions can be based on the following:

- File type
- File size
- File extension
- Digital signature
- Email (for Disarmer for Email only)

To define an exception:

1. From the navigation pane on the left, click **Policies**.
2. Click the case or file type you wish to define an exception for.
3. In the top right corner, click **Add Exception**.

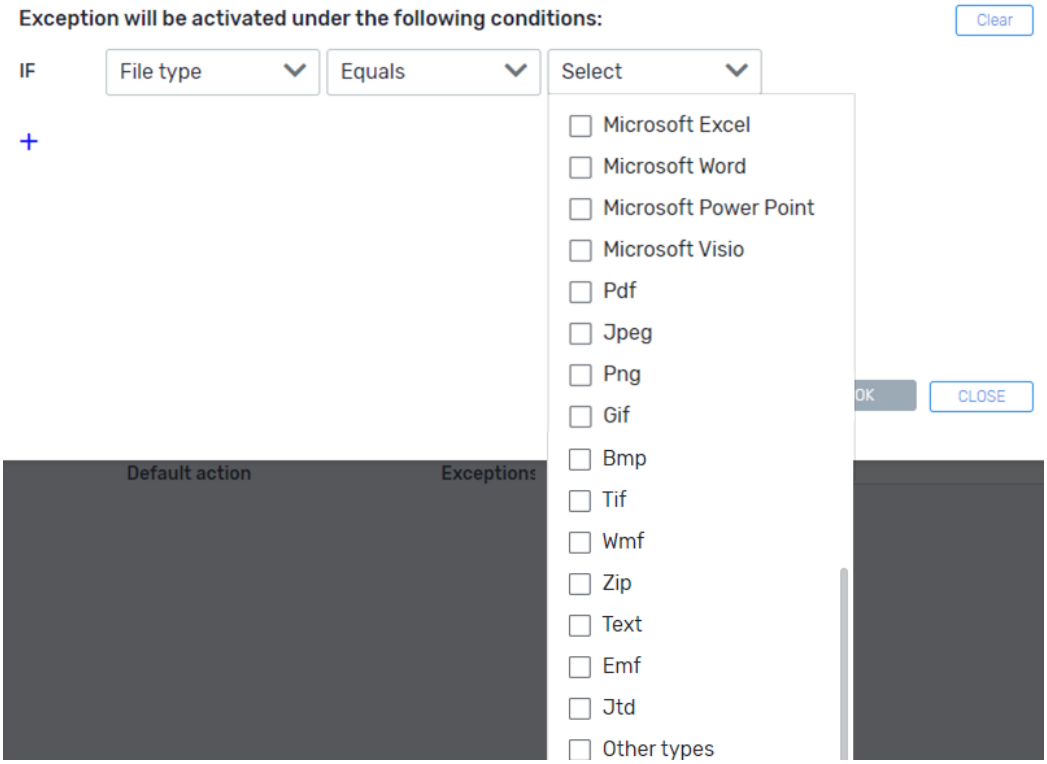
   The Define Exception window appears:



4. Define at least one condition to base the exception on. Create a condition by selecting values from the lists, or entering text, as appropriate.
5. To add another condition to the exception definition, click the **+** icon. To delete a condition, click the **X** icon.
6. To save the exception definition, click **OK**. You will return to the Policy page.

The exception is added to the right pane. You can further edit it or delete it, as needed.

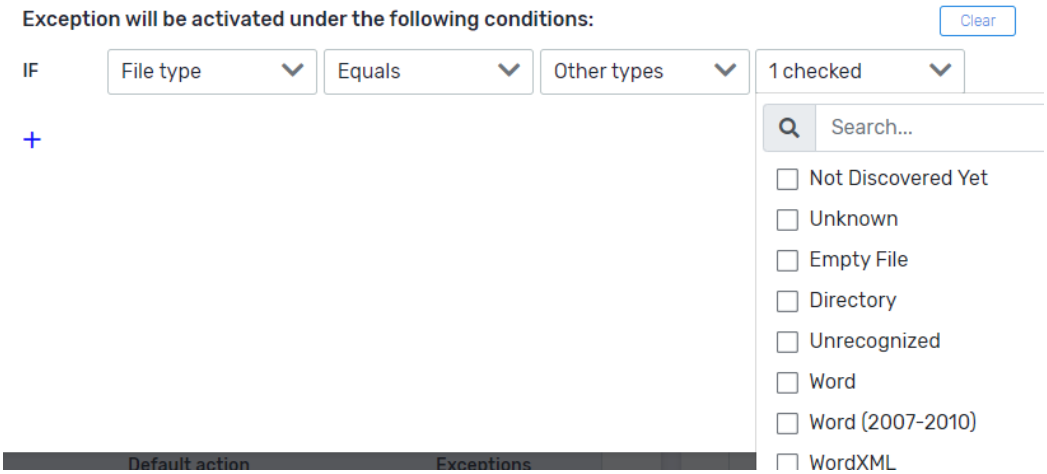
Defining Exceptions for File Types



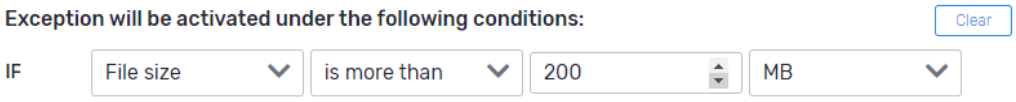
To specify an exception for one or more file types:

1. In the leftmost list, select **File Type**.
2. In the second list, select **Equals** or **Not Equals**.
3. In the last list, select one or more relevant file types. The list displays the most common ones.

To select a file type that does not appear in the list, select **Other types** (the last option in the list). An additional column appears. Enter search criteria and/or select one or more file types.



Defining Exceptions for File Size



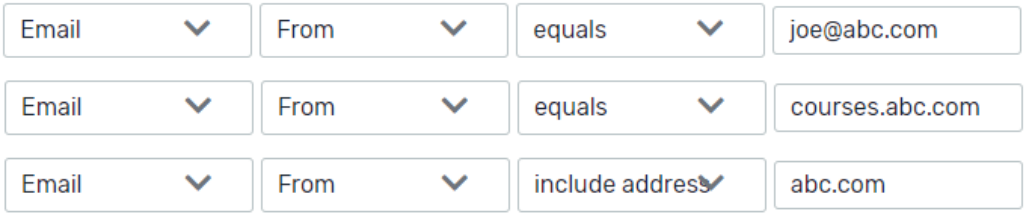
To specify an exception based on on file size:

1. In the leftmost list, select **File Size**.
2. In the second list, select **Is more than** or **Is less than**
3. In the file size definition field, use the up and down arrows, or enter a number.
4. In the last list, select from: Bytes, KB, MB, GB, or TB.

Note

- The file size entered is converted to bytes.

Defining Exceptions for Email Senders or Recipients



You can specify any of the following:

- From: For emails from a particular sender, or a specific domain.
- To: For emails to a particular recipient.
- CC: For emails to a particular CC-ed recipient.
- Recipients: For emails to recipients that appear in To, CC, or BCC fields.

Defining Email and Domain Addresses - Full and Partial

You can specify:

- An exact email or domain address by selecting **Equals** or **Not Equals**.
- A partial domain address by selecting **Include address**.

Guidelines and examples:

- Specify a full email address, including the **@** sign. For example, *joe@abc.com*.
- Partial email addresses are not accepted. For example, *@abc.com* or *joe@*.
- Specify full or partial domains. For example, *abc.com* or *courses.xyz.edu*

Defining Exceptions for File Extensions

To specify a list of file type extensions:

1. In the leftmost list, select **File Extension**.
2. In the second list, select **Ends with** or **Doesn't end with**.
3. In the text field, type in the extensions you need. Separate them with commas. For example: DOC,PDF,XLSX.

Defining Exceptions for Validating Signatures

You can specify an exception for a file that is signed either with a valid or invalid digital signature.

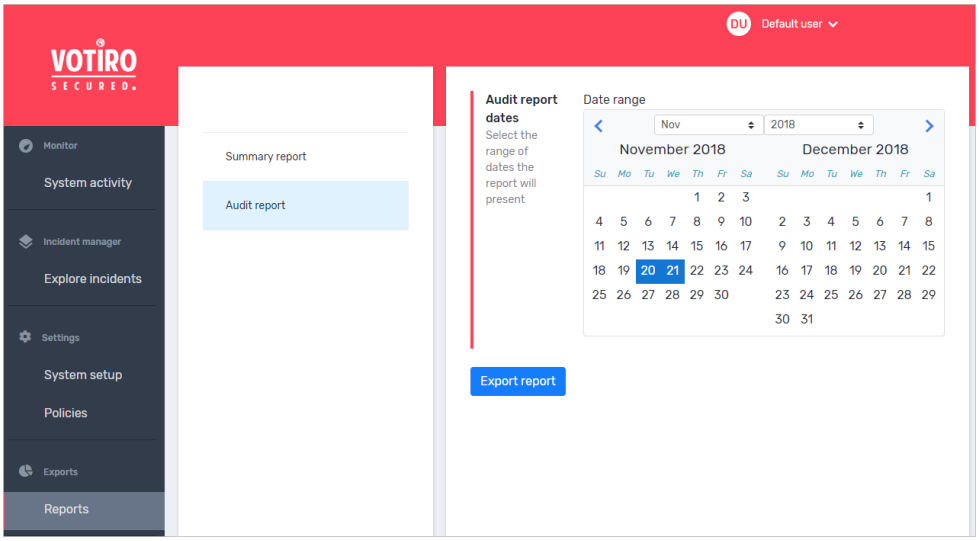
5.5 Auditing Actions Performed in the Management Platform

To protect enterprise privacy, Votiro tracks every login, change, request for file download and other actions that were performed in the Management Dashboard.

You can audit all actions that were performed by users of the Management Platform for a specified period. The exported report is a CSV file.

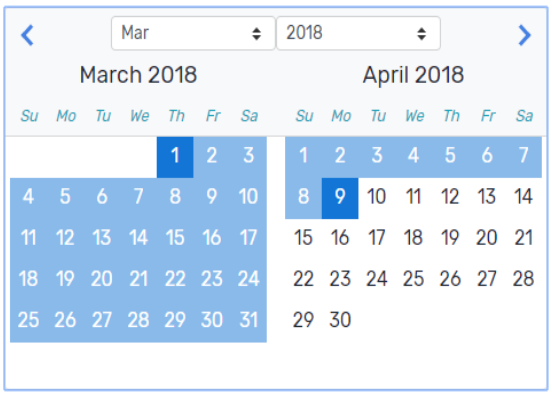
5.5.1 Generating an Audit

1. From the navigation pane on the left, click **Reports**.
2. Click **Audit report**.



3. In the period selector, navigate to the desired start month by clicking the right and left arrows or by selecting a month and year from the lists.
4. Click the start date.
5. Navigate to the desired end month.
6. Click the end date.

   The selected period is highlighted.



7. Click **Export Report**.

   The report is downloaded to your computer.

5.5.2 Audit Format and Structure

The audit is in CSV format. The following is an example excerpt as viewed in a spreadsheet application:

1/11/2018 11:52	RonF	LoginEvent	Successful login with Full permissions	
1/11/2018 13:05	user1	PolicyAddEvent	A new policy was created	policyId: 37a0add2-b521-442c-
1/11/2018 14:46	Default (unauthori	LoginEvent	Successful login with Full permis	
1/11/2018 15:07	RonF	LogoutEvent	Logout	
1/11/2018 15:41	Default (unauthori	LoginEvent	Successful login with Full permis	
1/11/2018 16:02	Default (unauthori	PolicyDeleteEvent	Policy 321_deleted_6367669212	policyId: 3d24ce9e-faca-4004-
1/11/2018 16:02	Default (unauthori	PolicyUpdateEvent	Policy jhg was changed	policyId: aab369db-32dd-4bad-
1/11/2018 16:03	Default (unauthori	ConfigurationEvent	3 Configuration record/s were u	updates:
1/11/2018 16:03	Default (unauthori	LogoutEvent	Logout	
1/11/2018 16:03	user1	LoginEvent	Successful login with Full permis	
1/11/2018 16:03	user1	UsersEvent	1 user/s permissions were upda	updates: Updated RonF from

Information is provided for the following actions:

- Login
- Logout
- Original file download
- Sanitized file download
- Release original
- Policy save
- Settings save
- Roles changes
- Report export
- Policy creation

For each action, there is a datestamp (in UTC time) and a username.

5.6 Generating a Summary Activity Report

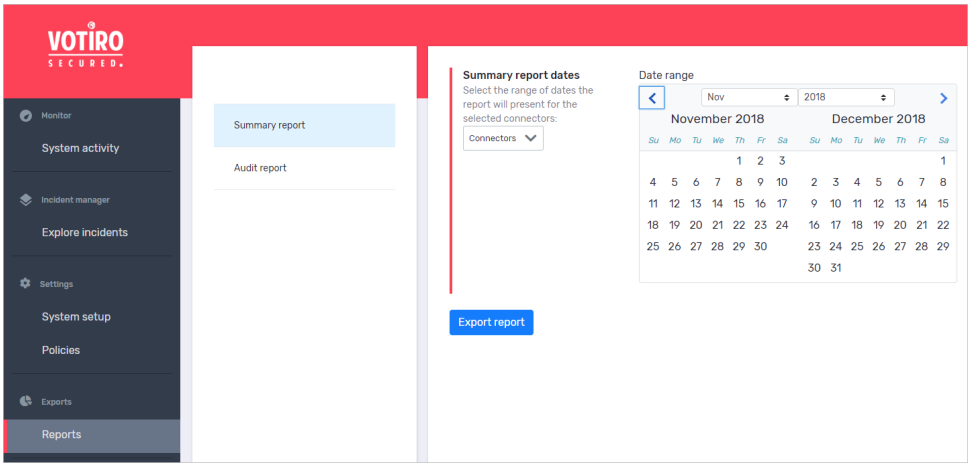
You can generate a summary report of the sanitization activity in your organization for a specified period.

The report collects useful data of the activity for all stakeholders. For example, the system administrator can use this report for making data-driven decisions to optimize the company's policy, for maximum security and minimum interference to your business.

The report presents usage and security date in graphic format and also provides tips for optimizing your sanitization effort.

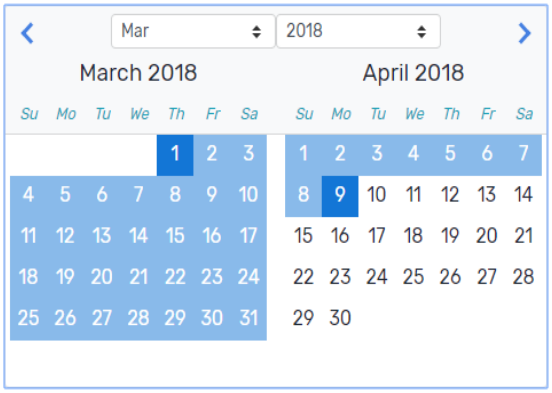
5.6.1 Generating a Report

1. In the navigation pane, click **Reports**.
2. Click **Summary report**.



3. From the **Connectors** list, select the connectors for which to generate the report.
4. In the period selector, navigate to the desired start month either by clicking the right and left arrows or by selecting a month and year from the lists.
5. Click the start date.
6. Navigate to the desired end month.
7. Click the end date.

   The selected period is highlighted.



8. Click **Export Report**.

   The report is downloaded to your computer.

5.6.2 Report Format and Structure

The report is in PDF format and provides the following information:

- Company name.
- Number of sanitization requests to Votiro Disarmer.
- Number of individual files that were sanitized by Disarmer.
- Number of files that were blocked.
- Number of threats that attempted to enter your organization.
- Number of files that were blocked according to each sanitization policy.
- Number of files that were blocked and that were detected as threats.
- Number of files that were blocked that were not threats.
- Average processing time in seconds/KB.
- File types that passed through Disarmer.
- Number of threats that attempted to enter your organization.
- Most threatening file types that were sent to your organization.

Appendix A Converting HTML to Text Emails

EML files that are written using HTML may contain malicious content and therefore many companies require them to be converted to text before they are sent to the recipient.

When activated, the policy handles the files in the following manner:

- The email attachments are preserved after the conversion.
- The email's body in plain text does not support bold, italic, colored fonts, or any other text formatting.
- Images and logos that are displayed directly in the message body are added as attachments to the sanitized email.
- In-line links, including in-line link images, are converted into URL addresses.
- Email body text is aligned from left to right.

> **Note**
> When an EML file contains calendar alternative content, which are not attachments, the email is not converted to plain text in order to preserve the invitation capabilities.

To activate this policy:

1. Click **Policies** in the Management navigation panel.
2. Click **Email** in the lists of Actions by File Types.
3. In the right panel, check **Convert HTML to Text**.
4. Click **Save**.

Appendix B Sending Logs to SIEM in CEF Format

In addition to the Disarmer logs that are configured in logs.xml, see Logs Settings on page 52. Disarmer logs can also be sent to SIEM in CEF format.

To enable SIEM logging, you must configure it in the report.xml file. The required configuration attributes are:

- **Log message format**: Must be CEF (default).
- **Address**: IP or hostname address for the Syslog server (default value = empty).
- **Port**: Syslog server port. Default port is 514.

An optional configuration attribute is:

- **AppName**: Scanner (default). The malware scanner sends antivirus update messages to SIEM.

> **Notes**
>
> - The IsActivated parameter under SiemSettings must be set to "true" in order for logs to be published.
> - For changes in the report.xml file to take effect, you must restart the Votiro.Sanitization.API and Votiro.SNMC Windows services.
> - For antivirus messages to be sent to SIEM, you must restart the Votiro Scanner service.

For more information see SIEM Report Settings on page 51

Here is an example of an SIEM message in the Disarmer system:

```
CEF:0|VOTIRO|SDS|7.2.0.289|20020100|Votiro Service Started|5|
rt=Sep 19 2017 05:57:38 dtz=03:00:00 dvchost=VOTIROSDSWS
msg=Votiro service started.
```

CEF Message Format

The CEF message format is as follows:

```
CEF:Version | Device Vendor | Device Product | Device Version |
Signature ID |Name |Severity | Date and host name extension
```

- **Version**. Always 0.
- **Device Vendor**: Always VOTIRO.
- **Device Product**: Always SDS.
- **Device Version**: The version of Disarmer.
- **Signature ID**: Event ID. Made up of Family Id and Id, where:
  - Family Id can be one of:

- 100, in the case of a Trace event.
- 200, in the case of a System event.
- 500, in the case of an Indicator event.
- 600, in the case of an Internal Trace event.

- Id is a five-numeral string.

- **Name**: Event Name indicates the type of event. See Report Events on the next page.
- **Severity**: Indicates the urgency of the event.

Table 21 Severity Levels

Level	Severity	Description
0	Verbose	Very fine-grained informational events that are most useful to debug an application.
1	Debug	Fine-grained informational events that are most useful to debug an application.
4	Info	Informational messages that highlight the progress of the application at coarse-grained level. This is the default level.
5	Notice	Informational messages that highlight the progress of the application at the highest level.
6	Warning	Potentially harmful situations.
7	Error	Error events that might still allow the application to continue running.
9	Fatal	Very severe error events that will presumably lead the application to abort.

- **Date and host name extension**. The rest of the extension follows these three values.
  - **Date**. Timestamp of event occurrence in the system. The extension always begins with three values:
    - rt = receipt time = time the message was first reported
    - dtz = device time zone = abbreviated. See: Time Zone Abbreviations.
    - dvchost is the host name, for example, John-PC
  - **Host name**. The name of the Disarmer server in which it occurred.
  - **Extension**. The last value is always msg, which stands for "message" and is the human readable message of the event description. See Report Events on the next page.

Report Events

Event codes respect the following 8-digit scheme:

LLRCCTTR

where L, R, C, T are digits [0-9].

- LL specifies the event main category.
- CC specifies the sub-category.
- TT specifies the specific event type.
- R is reserved for future use and must be ignored.

Examples

- 50020110 represents an Indicator event (LL=50) of category Suspicious Executable File (C=20), specifying that an executable artifact (TT=11) was found.
- 10000010 represents a Trace event (LL=10) of category FTD (C=00), specifying that a discovered file type (TT=01) was found.

Table 22 CEF Message Template Extensions

Category	Event Code	Sub-Category	Event Name	Event Description
Trace	10000010	File Type Discoverer	True File Type	File {FileName} recognized as {FileType}.
Trace	10010010	Antivirus	Antivirus Scan	File {FileName} successfully scanned by AV {AVEngine}.
Trace	10020100	File Process	File Uploaded	File {FileName} upload for sanitization started.
Trace	10020110	File Process	Sanitization Done	File {FileName} sanitization process successfully ended.
Trace	10020200	File Process	File Blocked	File {FileName} blocked as a result of the sanitization process.
Trace	10030100	API	API Limit Exceeded	File {FileName} upload request for sanitization exceeded the limit number of uploads.
Trace	10050100	Blocker	Block - Policy	File {FileName} blocked due to your organization policy violation {Policy} in the sanitization process.

Category	Event Code	Sub-Category	Event Name	Event Description
Trace	10050200	Blocker	Block - Antivirus	Virus found by {AVEngine} in file {FileName}.
Trace	10050300	Blocker	Block-Sandbox	Threat found by {SandboxName} in file {FileName}.
Trace	10050500	Blocker	Block - Error	File {FileName} blocked due to an error in Sanitization process.
Trace	10060100	Password Protected Opener	Password Opened	Password Protected File {FileName} successfully opened.
Trace	10060110	Password Protected Opener	Password Added	Password Protected File {FileName} successfully closes with original password.
Trace	10060200	Password Protected Opener	Wrong Password	Password Protected File {FileName} couldn't be opened.
Trace	10070010	Sandbox	Sandbox Scan	File {FileName} successfully scanned by {SandboxName}.
System	20010100	Antivirus	Antivirus Update Error	{AVEngine} signatures update process failed.
System	20010200	Antivirus	Antivirus Update	{AVEngine} signatures update process ended successfully.
System	20010300	Antivirus	Antivirus License Error	{AVEngine} license is invalid. License update is required.
System	20020000	Service	Votiro Service Starting	{ServiceName} is starting.
System	20020100	Service	Votiro Service Started	{ServiceName} service started.
System	20020110	Service	Votiro Service Stopped	{ServiceName} service stopped.
System	20030400	License	License Expired	License has expired, in {DaysToShutDown} days SDS will stop working, please renew your license.
System	20040500	UrlReputation	Url Connection Error	Url Reputation service {0} cannot be reached.

Category	Event Code	Sub-Category	Event Name	Event Description
System	20050600	Sandbox	Votiro Sandbox Service Error	Votiro sandbox service {SandboxName} cannot be reached.
System	20050700	Sandbox	Sandbox Service Error	Sandbox service {SandboxName} cannot be reached.
Indicator	50010000	Macro Analyzer	Suspicious Macro	Suspicious Office macro detected.
Indicator	50010010	Macro Analyzer	Suspicious Auto Execution Macro	Suspicious Office macro detected [Auto Execution].
Indicator	50010020	Macro Analyzer	Suspicious File System Activity Macro	Suspicious Office macro detected [File System Activity].
Indicator	50010030	Macro Analyzer	Suspicious Out Of Document Interaction Macro	Suspicious Office macro detected [Out-Of-Document Interaction].
Indicator	50010040	Macro Analyzer	Suspicious Office Excel 4.0 Macro	Suspicious Office Excel 4.0 macro detected.
Indicator	50020010	File Type Discoverer	Suspicious Fake File	Suspicious fake file [Extension does not match file structure] detected in the artifact.
Indicator	50020020	File Type Discoverer	Suspicious Unknown File	Unknown file [Data file or unidentified file type] detected in the artifact.
Indicator	50020110	File Type Discoverer	Suspicious Executable File	Executable file detected in the artifact.
Indicator	50020120	File Type Discoverer	Suspicious Script File	Script file detected in the artifact.
Indicator	50030100	AV	Suspicious Threat File	AV {AVEngine} detected a threat {ThreatType} in file {FileName}.
Indicator	50040010	Active Element	External Program Run Action	External Program Run Action detected in file {Filename}.
Indicator	50050010	JavaScript Analyzer	Dynamic code execution	Dynamic code execution detected in file {Filename}.
Indicator	50060010	Suspicious URL	Suspicious URL detected	Suspicious url detected in file {FileName}, URLs: {SuspiciousUrlsList}

Category	Event Code	Sub-Category	Event Name	Event Description
Indicator	50070050	Suspicious File Structure	Suspicious File Structure	Suspicious structure detected in file {FileName}
Indicator	50080100	Sandbox	Suspicious Sandbox Threat File	Sandbox engine {SandboxName} detected a threat ({ThreatName}) in file {FileName}.

Appendix C Windows Services Installed with Votiro Products

When Disarmer is installed on either Microsoft Windows Server 2012 or 2016, the following Windows services are installed:

- **Votiro.Sanitization.API**: this service is the gate to Disarmer for communications.
- **Votiro.Scanner**: this is an adapter used for AV scanning.
- **Votiro.SNMC**: the Sanitization Node Monitor Controller (SNMC) service is used to monitor your sanitization nodes.

When the Management Platform is installed on either Microsoft Windows Server 2012 or 2016, the following Windows services are installed:

- **Votiro.Blobs**: this service manages and stores both original and sanitized files.
- **Votiro.NotificationCenter**: this service listens to the votiro.notification queue and handles notifications by raising a ScanFileNotification to the votiro.scan queue.
- **Votiro.RetroScan**: this service listens to the votiro.scan queue and processes queued files. Following the initial scan on arrival, every 24 hours all files are re-scanned at days 1, 7 and 29. If a retrospectively scanned file is infected it is then sanitized.
- **Votiro.Scanner**: this is an adapter used for AV scanning.
- **Elasticsearch**: this service is used with the database of sanitized data.
- **Votiro.Audit**: this service monitors user activity and writes log files of activities with timestamp details.
- **Votiro.Sandbox**: this is a communication adapter between Disarmer and the third party sandbox.

Disarmer requires additional Windows Server features to function properly. They are installed automatically during the Disarmer engine installation:

- **.NET Framework 3.5 Features**
  - .NET Framework 3.5 (includes .NET 2.0 and 3.
    - WCF HTTP Activation
    - WCF Non-HTTP Activation
- **.NET Framework 4.5 Features (4.6 on Windows Server 2016)**
  - ASP.NET 4.5 (ASP.NET 4.6 on Windows Server 2016)
  - WCF Services
    - HTTP Activation

- Named Pipe Activation
- TCP Activation
- TCP Port Sharing

- **Internet Information Services** - World Wide Web Services
  - Application Development Feature
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5 (.NET Extensibility 4.6 on Windows Server 2016)
    - ASP.NET 4.5 (ASP.NET Extensibility 4.6 on Windows Server 2016
    - ISAPI Extensions
    - ISAPI Filters
  - Common HTTP Features
    - Default Document
  - Security
    - Basic Authentication
    - Request Filtering
    - Windows Authentication
- **Message Queuing**
  - Message Queuing Services
    - Message Queuing Server
    - Directory Service Integration
    - HTTP Support
    - Message Queuing Triggers
    - Routing Service
- **SNMP Service**
  - SNMP WMI Provider
- **Windows PowerShell**
  - Windows PowerShell 2.0 Engine
- **Windows Process Activation Service (WAS)**
  - NET Environment 3.5
  - Configuration APIs

- Process Model

As a result of the installation of the roles and features above, the following Windows services are installed on the host server.

- Application Host Helper Service
- ASP.NET State Service
- Windows Presentation Foundation Font Cache 3.0.0.0
- IIS Admin Service
- Net.Msmq Listener Adapter
- Net.Pipe Listener Adapter (in installations on Windows Server 2012 only)
- Net.Tcp Listener Adapter
- RPC/HTTP Load Balancing Service
- W3C Logging Service
- World Wide Web Publishing Service
- Windows Process Activation Service